On the Davenport-Heilbronn theorem and second order terms

Manjul Bhargava, Arul Shankar, and Jacob Tsimerman

June 1, 2010

1 Introduction

The classical theorem of Davenport and Heilbronn [15] provides an asymptotic formula for the number of cubic fields having bounded discriminant. Specifically, the theorem states:

Theorem 1 (Davenport–Heilbronn) *Let $N_3(\xi, \eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$
\begin{aligned}
N_3(0, X) &= \frac{1}{12\zeta(3)} X + o(X), \\
N_3(-X, 0) &= \frac{1}{4\zeta(3)} X + o(X).
\end{aligned}
\tag{1}
$$

The Davenport–Heilbronn theorem, and the methods underlying its proof, have seen applications in numerous works (see, e.g., [3], [4], [6], [11], [17], [18], [27], [28]).

Subsequent to their 1971 paper, extensive computations were undertaken by a number of authors (see, e.g., Llorente–Quer [21] and Fung–Williams [19]) in an attempt to numerically verify the Davenport–Heilbronn theorem. However, computations up to discriminants even as large as 10^7 were found to agree quite poorly with the theorem. This in turn led to questions about the magnitude of the error term in this theorem, and the problem of determining a precise second order term.

In a related work, Belabas [3] developed a method to enumerate cubic fields very fast—indeed, in essentially linear time with the discriminant—allowing him to make tables of cubic fields up to absolute discriminant 10^{11}. These computations still seemed to agree rather poorly with the Davenport–Heilbronn theorem, and led Belabas to only guess the existence of an error term smaller than $O(X/(\log X)^a))$ for any a. However, Belabas [2] later obtained the first subexponential error term of the form $O(X \exp(-\sqrt{\log X \log \log X}))$.

In 2000, Roberts [23] conducted a remarkable study of these latter computations in conjunction with certain theoretical considerations, which led him to conjecture a precise *second main term* in the Davenport–Heilbronn theorem. This conjectural second main term took the form of a certain explicit constant times $X^{5/6}$. Further computations carried out in the last few years have revealed Roberts' conjecture to agree extremely well with the data. Meanwhile, on the theoretical side, a power-saving error term was finally obtained by Belabas, the first author, and Pomerance [1], who showed an error term of $O(X^{7/8+\epsilon})$.

The purpose of the current article is to prove the above conjecture of Roberts. More precisely, we prove the following theorem.

Theorem 2 *Let $N_3(\xi, \eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$
\begin{aligned}
N_3(0, X) &= \frac{1}{12\zeta(3)} X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} X^{5/6} + O_\epsilon(X^{5/6-1/48+\epsilon}), \\
N_3(-X, 0) &= \frac{1}{4\zeta(3)} X + \frac{\sqrt{3} \cdot 4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} X^{5/6} + O_\epsilon(X^{5/6-1/48+\epsilon}).
\end{aligned}
\tag{2}
$$

Davenport and Heilbronn also proved a refined version of Theorem 1, where they give the asymptotics for the number of cubic fields K having bounded discriminant satisfying any specified set of splitting conditions at finitely many primes. Roberts also conjectures a precise second main term for the number of such fields K having discriminant bounded by X (see [23, Section 5]). We also prove Roberts' refined conjecture in Section 9.

In the process, we present a simpler approach to proving the original Davenport–Heilbronn theorem, and also a simpler approach to establishing the theorem of Davenport [14] on the density of discriminants of binary cubic forms. The second main term of the latter theorem of Davenport (who obtained only a second term of $O(X^{15/16})$) was first discovered by Shintani [26] using Sato and Shintani's theory of zeta functions for prehomogeneous vector spaces [25]. In this article, we also give an elementary derivation of this second main term of Shintani. More precisely, we prove:

Theorem 3 (Davenport–Shintani) *Let $N(\xi, \eta)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integer-coefficient binary cubic forms f satisfying $\xi < \mathrm{Disc}(f) < \eta$. Then*

$$
\begin{aligned}
N(0, X) &= \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{15\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
N(-X, 0) &= \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{5\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
\tag{3}
$$

In order to prove Theorem 2, we need (in particular) to apply a new, stronger version of Theorem 3 where we count equivalence classes of binary cubic forms satisfying any finite or other suitable set of congruence conditions. Such a theorem was obtained by Davenport–Heilbronn but their method does not yield second main terms. Meanwhile, Shintani's zeta function method does not immediately apply to cubic forms satisfying given congruence conditions. We prove this congruence version of Theorem 3 in Section 6.

In fact, we use this more general version of Theorem 3 to prove a generalization of Theorem 2 that also allows us to count cubic orders satisfying certain specified sets of local conditions. To state this more general theorem, we first restate Theorem 3 as:

Theorem 4 *Let $M_3(\xi, \eta)$ denote the number of isomorphism classes of orders R in cubic fields that satisfy $\xi < \mathrm{Disc}(R) < \eta$. Then*

$$
\begin{aligned}
M_3(0, X) &= \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{15\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
M_3(-X, 0) &= \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{5\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
\tag{4}
$$

The proof of Theorem 4 is relatively straightforward, given Theorem 3 and the "Delone–Faddeev bijection" between isomorphism classes of cubic orders and $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms (which we describe in more detail in Section 2).

The generalization of Theorem 2 (which will also then include Theorem 4) that we will prove allows one to count cubic orders of bounded discriminant satisfying any desired finite (or, in many natural cases, infinite) sets of local conditions. To state the theorem, for each prime p let Σ_p be any set of isomorphism classes of orders in étale cubic algebras over $\mathbb{Q}_p$; also, let Σ_∞ denote any set of isomorphism classes of étale cubic algebras over $\mathbb{R}$ (i.e., $\Sigma_\infty \subseteq \{\mathbb{R}^3, \mathbb{R} \oplus \mathbb{C}\}$). We say that the collection $(\Sigma_p) \cup \Sigma_\infty$ is *acceptable* if, for all sufficiently large primes p, the set Σ_p contains all maximal cubic orders over $\mathbb{Z}_p$—or at least those maximal cubic orders that are not totally ramified. We say that the collection $(\Sigma_p) \cup \Sigma_\infty$ is *strongly acceptable* if, for all sufficiently large primes p, the set Σ_p either consists of the set all maximal cubic orders over $\mathbb{Z}_p$ or the set of all cubic orders over $\mathbb{Z}_p$.

We wish to asymptotically count the total number of cubic orders R of absolute discriminant less than X that agree with such local specifications, i.e., $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. This asymptotic count—with the first *two* main terms—is contained in the following theorem:

Theorem 5 *Let $(\Sigma_p) \cup \Sigma_\infty$ be a strongly acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. For a free $\mathbb{Z}_p$-module M, define $M^{\mathrm{Prim}} \subset M$ by $M^{\mathrm{Prim}} := M \backslash \{p \cdot M\}$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$
N_3(\Sigma; X) = \Big(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|}\Big) \cdot \prod_p \Big(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|}\Big) \cdot X
$$

$$
+ \quad \frac{1}{\zeta(2)} \Big(\sum_{R \in \Sigma_\infty} c_2(R)\Big) \cdot \prod_p \Big((1 - p^{-1/3}) \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3} dx\Big) \cdot X^{5/6}
$$

$$
+ \quad O_\epsilon(X^{5/6 - 1/48 + \epsilon}),
$$

(5)

where $\mathrm{Disc}_p(R)$ denotes the discriminant of R over $\mathbb{Z}_p$ as a power of p, $i(x)$ denotes the index of $\mathbb{Z}_p[x]$ in R, dx assigns measure 1 to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$, and

$$
c_2(R) = \begin{cases} c_2^{(0)} := \dfrac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{15\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}, \\[3mm] c_2^{(1)} := \dfrac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{5\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{C}. \end{cases}
$$

Note that the case where Σ_p consists of the maximal cubic orders over $\mathbb{Z}_p$ for all p yields Theorem 1, and also yields a corresponding interpretation of the asymptotic constants in Theorem 1 as a product of local Euler factors. Indeed, these Euler factors correspond to local weighted counts of the possible cubic algebras that can arise over $\mathbb{Q}_p$ and over $\mathbb{Q}_\infty = \mathbb{R}$.

Meanwhile, the case where Σ_p consists of all orders in étale cubic algebras over $\mathbb{Q}_p$ yields Theorem 4, and again also yields the analogous interpretation of the constants in Theorem 4. Theorem 5 thus simultaneously generalizes Theorems 2 and 4 in a natural way, and moreover, it yields a natural interpretation of the various constants $\frac{\pi^2}{72}$, $\frac{\pi^2}{24}$, $\frac{1}{12\zeta(3)}$, $\frac{1}{4\zeta(3)}$, etc. that appear in the asymptotics of these theorems.

If we are only interested in the first main term, we have the following stronger result:

Theorem 6 *Let $(\Sigma_p) \cup \Sigma_\infty$ be an acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Q}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$
N_3(\Sigma; X) = \Big(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|}\Big) \cdot \prod_p \Big(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|}\Big) \cdot X + o(X). \tag{6}
$$

The case where, for all p, the set Σ_p consists of all maximal cubic rings that are not totally ramified at p yields the following corollary which is also due to Davenport and Heilbronn.

Corollary 7 *Let D denote the discriminant of a quadratic field and let $\mathrm{Cl}_3(D)$ denote the 3-torsion subgroup of the ideal class group $\mathrm{Cl}(D)$ of D. Then*

$$
\lim_{X \to \infty} \frac{\sum_{0 < D < X} \#\mathrm{Cl}_3(D)}{\sum_{0 < D < X} 1} = \frac{4}{3}, \qquad \lim_{X \to \infty} \frac{\sum_{-X < D < 0} \#\mathrm{Cl}_3(D)}{\sum_{-X < D < 0} 1} = 2.
$$

Our proofs of Theorems 1–6 and particularly Theorem 5, though perhaps similar in spirit to the original arguments of Davenport and Heilbronn, involve a number of new ideas and refinements both on the algebraic and the analytic side. First, we begin in Sections 2 and 3 by giving a much shorter and more elementary derivation of the "Davenport–Heilbronn correspondence" between maximal cubic orders and appropriate sets of binary cubic forms.

Second, we obtain the main term of the asymptotics of Theorem 3 in Section 5 by counting points not in a single fundamental domain, but on average in a continuum of fundamental domains, using a technique of [7]. This leads, in particular, to a uniform treatment of the cases of positive and negative discriminants. It also leads directly to stronger error terms; most notably, we obtain immediately an error term of $O(X^{5/6})$ for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms of discriminant less than X, improving on Davenport's original $O(X^{15/16})$. The $O(X^{5/6})$ term is seen to come from the "cusps" or "tentacles" of the fundamental regions.

Third, to more efficiently count points in the cusps of these fundamental regions, we introduce a "slicing and smoothing" technique in Section 6, which then allows us to keep track of precise second order terms and thus also prove the second main term of Theorem 3. The technique works equally well when counting points satisfying any finite set of congruence conditions (see Theorem 21).

Fourth, our use of the Delone–Faddeev correspondence (c.f. Section 2) allows us to give an elementary treatment of the analogue of Theorem 2 for orders, rather than just fields, as in Theorem 4 and in the cases of Theorem 5 where only finitely many local conditions are involved. We prove the main terms of Theorems 1–6 in Section 8, using a simplified computation of p-adic densities that is carried out in Section 4.

Finally—in order to treat the second term in cases where infinitely many local conditions are involved—we introduce a sieving method that allows one to preserve the second main terms even when certain natural infinite sets of congruence conditions are applied. This is accomplished in Section 9, using a computation of "second order p-adic densities" that is carried out in Section 7.

Remark. Readers interested only in our new simpler proofs of the main terms of the Davenport–Heilbronn theorems may safely skip Sections 6, 7 and 9, which constitute about a half of this paper. On the other hand, those interested in the new results on second main terms may wish to concentrate primarily on these sections.

2   The Delone–Faddeev correspondence

A *cubic ring* is any commutative ring with unit that is free of rank 3 as a $\mathbb{Z}$-module. We begin with a theorem of Delone–Faddeev [16] (as refined by Gan–Gross–Savin [20]) parametrizing cubic rings by $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms. Throughout this paper, we always use the "twisted" action of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms, i.e., an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x,y)$ by

$$(\gamma \cdot f)(x,y) = \frac{1}{\det(\gamma)} \cdot f((x,y) \cdot \gamma).$$

Theorem 8 ([16],[20]) *There is a natural bijection between the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings.*

Proof: Given a cubic ring R, let $\langle 1, \omega, \theta \rangle$ be a $\mathbb{Z}$-basis for R. Translating ω, θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega \cdot \theta \in \mathbb{Z}$. A basis satisfying the latter condition is called *normal*. If $\langle 1, \omega, \theta \rangle$ is a normal basis, then there exist constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$
\begin{aligned}
\omega\theta &= n \\
\omega^2 &= m + b\omega - a\theta \\
\theta^2 &= \ell + d\omega - c\theta.
\end{aligned}
\tag{7}
$$

To the cubic ring R, associate the binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (7). The values of ℓ, m, n are subject to the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega \cdot \omega\theta$, which when multiplied out using (7), yield a system of equations that possess a unique solution for n, m, ℓ, namely

$$
\begin{aligned}
n &= -ad \\
m &= -ac \\
\ell &= -bd.
\end{aligned}
\tag{8}
$$

4

If follows that any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (7) and (8), leads to a unique cubic ring $R = R(f)$.

Lastly, one observes by an explicit calculation that changing the $\mathbb{Z}$-basis $\langle \omega, \theta \rangle$ of $R/\mathbb{Z}$ by an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the corresponding binary cubic form $f(x, y)$ by that same element of $\mathrm{GL}_2(\mathbb{Z})$. Hence an isomorphism class of cubic rings determines a binary cubic form uniquely up to the action of $\mathrm{GL}_2(\mathbb{Z})$. This is the desired conclusion. $\square$

One finds by an explicit calculation using (7) and (8) that *the discriminant of the cubic ring $R(f)$ is precisely the discriminant of the binary cubic form f*; explicitly, it is given by

$$\mathrm{Disc}(R(f)) = \mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \qquad (9)$$

Next, we observe that *the cubic ring $R(f)$ is an integral domain if and only if f is irreducible as a polynomial over $\mathbb{Q}$*. Indeed, if $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is reducible, then it has a linear factor, which (by a change of variable in $\mathrm{GL}_2(\mathbb{Z})$) we may assume is y; i.e., $a = 0$. In this case, (7) and (8) show that $\omega\theta = 0$, so $R(f)$ has zero divisors.

Conversely, if a cubic ring R has zero divisors, then there exists some element $\omega \in R$ such that $\langle 1, \omega \rangle$ spans a quadratic subring of R. Such an ω can be constructed as follows. Let α and β be two nonzero elements of R with $\alpha\beta = 0$, and let $\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$ be the characteristic polynomial of α. Multiplying both sides by β, we see that $c_3 = 0$, so that $\alpha(\alpha^2 + c_1\alpha + c_2) = 0$. If $\alpha^2 + c_1\alpha + c_2 = 0$, then we may let $\omega = \alpha$. Otherwise, note that $(\alpha^2 + c_1\alpha + c_2)^2 = c_2(\alpha^2 + c_1\alpha + c_2)$, so in that case we may set $\omega = \alpha^2 + c_1\alpha + c_2$, and $\omega^2 = c_2\omega$. Either way, we see that $\langle 1, \omega \rangle$ spans a quadratic subring of R.

Scaling ω by an integer if necessary, we may assume that ω is a primitive vector in the lattice $R \cong \mathbb{Z}^3$, and then extend $\langle 1, \omega \rangle$ to a basis $\langle 1, \omega, \theta \rangle$ of R. Normalizing this basis if needed, we then see in (7) that we must have $a = 0$, implying that the associated binary cubic form is reducible. We conclude that, under the Delone–Faddeev correspondence, integral domains correspond to irreducible binary cubic forms.

Other properties of the cubic ring $R(f)$ can also be read off easily from the binary cubic form f. For example, *the group of ring automorphisms of $R(f)$ is simply the stabilizer of f in $\mathrm{GL}_2(\mathbb{Z})$*; this follows directly from the proof of Theorem 8.

Finally, we note that the correspondence of Theorem 8, and the analogues of the above consequences, also hold for cubic algebras and binary cubic forms over other base rings such as $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, and $\mathbb{Z}_p$, with the identical proofs. This observation will also be very useful to us in later sections.

3   The Davenport–Heilbronn correspondence

A cubic ring is said to be *maximal* if it is not a subring of any other cubic ring. The first part of the Davenport–Heilbronn theorem [15] describes a bijection (known as the "Davenport–Heilbronn correspondence") between maximal cubic rings and certain special classes of binary cubic forms. In this section, we give a simple derivation of this bijection.

By the work of the previous section, in order to obtain the Davenport–Heilbronn correspondence we must simply determine which binary cubic forms f yield maximal rings $R(f)$ in the bijection given by (7) and (8). Now a cubic ring R is maximal if and only if the cubic $\mathbb{Z}_p$-algebra $R_p = R \otimes \mathbb{Z}_p$ is maximal for every p (this is because R is a maximal ring if and only if it is isomorphic to a product of rings of integers in number fields). The condition on R that $R \otimes \mathbb{Z}_p$ be a maximal cubic algebra over $\mathbb{Z}_p$ is called "maximality at p". The following lemma illustrates the ways in which a ring R can fail to be maximal at p:

Lemma 9 *Suppose R is not maximal at p. Then there is a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ of R such that at least one of the following is true:*

- *$\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ forms a ring*

- *$\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ forms a ring.*

Proof: Let $R' \supset R$ be any ring strictly containing R such that the index of R in R' is a multiple of p, and let $R_1 = R' \cap (R \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}])$. Then the ring R_1 also strictly contains R, and the index of R in R_1 is a power of p. By the theory of elementary divisors, there exist nonnegative integers $i \geq j$ and a basis $\langle 1, \omega, \theta \rangle$ of R such that

$$R_1 = \mathbb{Z} + \mathbb{Z}(\omega/p^i) + \mathbb{Z}(\theta/p^j). \tag{10}$$

If $i = 1$, we are done. Hence we assume $i > 1$.

We normalize the basis $\langle 1, \omega, \theta \rangle$ if necessary; this does not affect the truth of equation (10). Now suppose the multiplicative structure of R is given by (7) and (8). That the right side of (10) is a ring translates into the following congruence conditions on a, b, c, d:[1]

$$a \equiv 0 \pmod{p^{2i-j}}, \quad b \equiv 0 \pmod{p^i}, \quad c \equiv 0 \pmod{p^j}, \quad d \equiv 0 \pmod{p^{2j-i}}. \tag{11}$$

If $j = 0$, then replacing (i, j) by $(i - 1, j)$ maintains the truth of the above congruences, and R_1 as defined by (10) remains a ring. If $j > 0$, then we may replace (i, j) instead by $(i - 1, j - 1)$. Thus in a finite sequence of such moves, we arrive at $i = 1$, as desired. $\square$

The lemma implies that a cubic ring $R(f)$ can fail to be maximal at p in two ways: either (i) f is a multiple of p, or (ii) there is some $\mathrm{GL}_2(\mathbb{Z})$-transformation of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ such that a is a multiple of p^2 and b is a multiple of p.

Let $\mathcal{U}_p$ be the set of all binary cubic forms f not satisfying either of the latter two conditions. Then we have proven

Theorem 10 (Davenport–Heilbronn [15]) *The cubic ring $R(f)$ is maximal if and only if $f \in \mathcal{U}_p$ for all p.*

Note that our definition of $\mathcal{U}_p$ is somewhat simpler than that used by Davenport–Heilbronn (but is easily seen to be equivalent).

4 Local behavior and p-adic densities

In this section, we consider elements f in the spaces of binary cubic forms f over the integers $\mathbb{Z}$, the p-adic ring $\mathbb{Z}_p$, and the residue field $\mathbb{Z}/p\mathbb{Z}$. We denote these spaces by $V_{\mathbb{Z}}$, $V_{\mathbb{Z}_p}$, and $V_{\mathbb{F}_p}$ respectively.

Aside from the degenerate case $f \equiv 0 \pmod{p}$, any form $f \in V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) determines exactly three points in $\mathbb{P}^1_{\mathbb{F}_p}$, obtained by taking the roots of f reduced modulo p. For such a form f, define the symbol (f, p) by setting

$$(f, p) = (f_1^{e_1} f_2^{e_2} \cdots),$$

where the f_i's indicate the degrees of the fields of definition over $\mathbb{F}_p$ of the roots of f, and the e_i's indicate the respective multiplicities of these roots. There are thus five possible values of the symbol (f, p), namely, (111), (12), (3), $(1^2 1)$, and (1^3). Furthermore, it is clear that if two binary cubic forms f_1, f_2 over $\mathbb{Z}$ (resp. $\mathbb{Z}_p$, $\mathbb{F}_p$) are equivalent under a transformation in $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$), then $(f_1, p) = (f_2, p)$. By $T_p(111), T_p(12)$, etc., let us denote the set of f such that $(f, p) = (111)$, $(f, p) = (12)$, etc.

By the definition of $R(f)$, the ring structure of the quotient ring $R(f)/(p)$ depends only on the $\mathrm{GL}_2(\mathbb{F}_p)$-orbit of f modulo p; hence the symbol (f, p) indicates something about the structure of the ring $R(f)$ when reduced modulo p. In fact, writing down the multiplication laws at one point of each of the five aforementioned $\mathrm{GL}_2(\mathbb{F}_p)$-orbits demonstrates that

$$(f, p) = (f_1^{e_1} f_2^{e_2} \cdots) \iff R(f)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots.$$

In particular, it follows that for $f \in \mathcal{U}_p$, the symbol (f, p) conveys precisely the splitting behavior of $R(f)$ at p. For example, if $(f, p) = (1^3)$ for $f \in \mathcal{U}_p$, then this means the maximal cubic ring $R(f)$ is totally ramified at p.

Now, for any set S in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) that is definable by congruence conditions, let us denote by $\mu(S) = \mu_p(S)$ the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ on V so that $\mu(V_{\mathbb{Z}_p}) = 1$. The following lemma determines the p-adic densities of the sets $T_p(\cdot)$:

---

[1] We follow here the convention that, for $e \leq 0$, we have $a \equiv 0 \pmod{p^e}$ for any integer a.

Lemma 11 *We have*

$$
\begin{aligned}
\mu(T_p(111)) &= \tfrac{1}{6}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(12)) &= \tfrac{1}{2}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(3)) &= \tfrac{1}{3}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(1^2 1)) &= \quad (p-1)\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(1^3)) &= \quad (p-1)\,(p+1)\,/\,p^4
\end{aligned}
$$

Proof: Since the criteria for membership of f in a $T_p(\cdot)$ depend only on the residue class of f modulo p, it suffices to consider the situation over $\mathbb{F}_p$. We examine first $\mu(T_p(111))$. The number of unordered triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is $\tfrac{1}{6}(p+1)p(p-1)$. Furthermore, given such a triple of points, there is a unique binary cubic form, up to scaling, having this triple of points as its roots. Since the total number of binary cubic forms over $\mathbb{F}_p$ is p^4, it follows that $\mu(T_p(111)) = \tfrac{1}{6}\big[(p+1)p(p-1)\big](p-1)/\,p^4$, as given by the lemma.

Similarly, the number of unordered triples of points, one member of which is in $\mathbb{P}^1_{\mathbb{F}_p}$ while the other two are $\mathbb{F}_p$-conjugate in $\mathbb{P}^1_{\mathbb{F}_{p^2}}$, is given by $\tfrac{1}{2}(p+1)(p^2-p)$. We thus have $\mu(T_p(12)) = \tfrac{1}{2}\big[(p+1)(p^2-p)\big](p-1)/\,p^4$. Also, the number of unordered $\mathbb{F}_p$-conjugate triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_{p^3}}$ is $(p^3-p)/3$, and hence $\mu(T_p(3)) = \big[(p^3-p)\big](p-1)/\,p^4$.

Meanwhile, the number of pairs (x,y) of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is given by $(p+1)p$, so that the number of binary cubic forms over $\mathbb{F}_p$ having a double root at some point x and a single root at another point y is $[(p+1)p](p-1)$. Thus $\mu(T_p(1^2 1)) = \big[(p+1)p\big](p-1)/\,p^4$. Finally, the number of binary cubic forms over $\mathbb{F}_p$ having a triple root in $\mathbb{P}^1_{\mathbb{F}_p}$ is $(p+1)(p-1)$, yielding $\mu(T_p(1^3)) = (p+1)(p-1)/p^4$ as desired. $\square$

We next wish to determine the p-adic densities of the sets $\mathcal{U}_p$. Let $\mathcal{U}_p(\cdot)$ denote the subset of elements $f \in T_p(\cdot)$ such that $R(f)$ is maximal at p. If f is an element of $T_p(111)$, $T_p(12)$, or $T_p(3)$, then $R(f)$ is clearly maximal at p, as its discriminant is coprime to p. Thus $U_p(111) = T_p(111)$, $U_p(12) = T_p(12)$, and $U_p(3) = T_p(3)$. If a binary cubic form f is in $T_p(1^2 1)$ or $T_p(1^3)$, then it can clearly be brought into the form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $a \equiv b \equiv 0 \pmod{p}$, namely, by sending the unique multiple root of f in $\mathbb{P}^1_{\mathbb{F}_p}$ to the point $(1,0)$ via a transformation in $\mathrm{GL}_2(\mathbb{Z})$. Of all $f \in T_p(1^2 1)$ or $T_p(1^3)$ that have been rendered in such a form, a proportion of $1/p$ actually satisfy the congruence $a \equiv 0 \pmod{p^2}$ of condition (ii). Thus a proportion of $(p-1)/p$ of forms in $T_p(1^2 1)$ and in $T_p(1^3)$ correspond to cubic rings maximal at p. We have thus proven:

Lemma 12 *We have*

$$
\begin{aligned}
\mu(\mathcal{U}_p(111)) &= \tfrac{1}{6}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(12)) &= \tfrac{1}{2}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(3)) &= \tfrac{1}{3}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(1^2 1)) &= \quad (p-1)^2\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(1^3)) &= \quad (p-1)^2\,(p+1)\,/\,p^5\,.
\end{aligned}
$$

Following [15] let $\mathcal{V}_p$ denote the set of elements $f \in \mathcal{U}_p$ such that $(f,p) \neq (1^3)$. Then it is clear from the above arguments that the elements of $\mathcal{V}_p$ correspond to maximal orders in étale cubic algebras over $\mathbb{Q}$ in which p does not totally ramify. The set $\mathcal{V}_p$ plays an important role in understanding the 3-torsion in the class groups of cubic fields (see Section 8).

Using the fact that $\mathcal{U}_p$ is simply the union of the $\mathcal{U}_p(\sigma)$'s, and $\mathcal{V}_p$ is the union of the $\mathcal{U}_p(\sigma)$'s where $\sigma \neq (1^3)$, we obtain from Lemma 12:

Lemma 13 *We have*

$$
\begin{aligned}
\mu(\mathcal{U}_p) &= (p^3-1)(p^2-1)\,/\,p^5 \\
\mu(\mathcal{V}_p) &= (p^2-1)^2\,/\,p^4\,.
\end{aligned}
$$

5 The number of binary cubic forms of bounded discriminant

Let $V = V_{\mathbb{R}}$ denote the vector space of binary cubic forms over $\mathbb{R}$. Then the action of $\mathrm{GL}_2(\mathbb{R})$ on V has two nondegenerate orbits, namely the orbit $V^{(0)}$ consisting of elements having positive discriminant, and $V^{(1)}$ consisting of those having negative discriminant. In this section we wish to understand the number $N(V^{(i)}; X)$ of <u>irreducible</u> $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i)}$ having absolute discriminant less than X ($i = 0, 1$). In particular, we prove the following strengthening of Davenport's theorem on the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms having bounded discriminant:

Theorem 14 $N(V_{\mathbb{Z}}^{(0)}; X) = \dfrac{\pi^2}{72} \cdot X + O(X^{5/6})$; $N(V_{\mathbb{Z}}^{(1)}; X) = \dfrac{\pi^2}{24} \cdot X + O(X^{5/6})$.

5.1 Reduction theory

Let $\mathcal{F}$ denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$. Then $\mathcal{F}$ may be expressed in the form $\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', k \in K, \lambda \in \Lambda\}$, where

$$N'(a) = \{\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} : n \in \nu(a)\}, \quad A' = \{\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2}\}, \quad \Lambda = \{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0\} \quad (12)$$

and K is as usual the (compact) real special orthogonal group $\mathrm{SO}_2(\mathbb{R})$; here $\nu(a)$ is the union of either one or two subintervals of $[-\frac{1}{2}, \frac{1}{2}]$ depending only on the value of $a \in A'$.

For $i = 1, 2$, let n_i denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any element $v \in V_{\mathbb{R}}^{(i)}$ (by the correspondence of Theorem 8 over $\mathbb{R}$, we have $n_1 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^3) = 6$ and $n_2 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = 2$). Then for any $v \in V^{(i)}$, $\mathcal{F}v$ will be the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$. Since this union is not necessarily disjoint, $\mathcal{F}v$ is best viewed as a multiset, where the multiplicity of a point x in $\mathcal{F}v$ is given by the cardinality of the set $\{g \in \mathcal{F} \mid gv = x\}$. Evidently, this multiplicity is a number between 1 and n_i.

Even though the multiset $\mathcal{F}v$ is the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$, not all elements in $\mathrm{GL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}$ will be represented in $\mathcal{F}v$ exactly n_i times. In general, the number of times the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of an element $x \in V_{\mathbb{Z}}$ will occur in the multiset $\mathcal{F}v$ is given by $n_i/m(x)$, where $m(x)$ denotes the size of the stabilizer of x in $\mathrm{GL}_2(\mathbb{Z})$. Now the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an irreducible element $x \in V_{\mathbb{Z}}$ is either trivial or C_3. We conclude that, for any $v \in V_{\mathbb{R}}^{(i)}$, the product $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$ is exactly equal to the number of irreducible integer points in $\mathcal{F}v$ having absolute discriminant less than X, with the slight caveat that the (relatively rare—see Lemma 16) C_3-points are to be counted with weight $1/3$.

Now the number of such integer points can be difficult to count in a single such fundamental domain. The main technical obstacle is that the fundamental region $\mathcal{F}v$ is not compact, but rather has a cusp going off to infinity which in fact contains infinitely many points, including many irreducible points. We simplify the counting of such points by "thickening" the cusp; more precisely, we compute the number of points in the fundamental region $\mathcal{F}v$ by averaging over lots of such fundamental domains, i.e., by averaging over points v lying in a certain special compact subset B of some fixed ball in V.

5.2 Estimates on reducibility

We first consider the reducible elements in the multiset $\mathcal{R}_X(v) := \{w \in \mathcal{F}v : |\mathrm{Disc}(w)| < X\}$, where v is any vector in a fixed compact subset B of V. Note that if a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3$ satisfies $a = 0$, then it is reducible over $\mathbb{Q}$, since y is a factor. The following lemma shows that for binary cubic forms in $\mathcal{R}_X(v)$, reducibility with $a \neq 0$ does not occur very often.

Lemma 15 *Let $v \in B$ be any point of nonzero discriminant, where B is any fixed compact subset of V. Then the number of integral binary cubic forms $ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{R}_X(v)$ that are reducible with $a \neq 0$ is $O(X^{3/4+\epsilon})$, where the implied constant depends only on B.*

Proof: For an element $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{R}_X(v)$, we see via the description of $\mathcal{R}_X(v)$ as $N'A'K\Lambda v$, where $v \in B$ and $0 < \lambda < X^{1/4}$, that $a = O(X^{1/4})$, $ab = O(X^{1/2})$, $ac = O(X^{1/2})$, $ad = O(X^{1/2})$, $abc = O(X^{3/4})$, and $abd = O(X^{3/4})$. In particular, the latter estimates clearly imply that the total number of forms $f \in \mathcal{R}_X(v)$ with $a \neq 0$ and $d = 0$ is $O(X^{3/4+\epsilon})$.

Let us now assume $a \neq 0$ and $d \neq 0$. Then the above estimates show that the total number of possibilities for the triple (a, b, d) is $O(X^{3/4+\epsilon})$. Suppose the values a, b, d $(d \neq 0)$ are now fixed, and consider the possible number of values of c such that the resulting form $f(x, y)$ is reducible. For $f(x, y)$ to be reducible, it must have some linear factor $rx + sy$, where $r, s \in \mathbb{Z}$ are relatively prime. Then r must be a factor of a, while s must be a factor of d; they are thus both determined up to $O(X^\epsilon)$ possibilities. Once r and s are determined, computing $f(-s, r)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a, b, d, r, s. Thus the total number of reducible forms $f \in \mathcal{R}_X(v)$ with $a \neq 0$ is $O(X^{3/4+\epsilon})$, as desired. $\square$

Lemma 16 *Let $v \in V$ be any point of positive discriminant. Then the number of C_3-points in $\mathcal{R}_X(v)$ is $O(X^{3/4+\epsilon})$, where the implied constant is independent of V.*

Proof: The number of C_3-points in $\mathcal{R}_X(v)$ is equal to the number of isomorphism classes of cubic rings having automorphism group C_3 and discriminant less than X. This number is thus independent of v, and so it suffices to prove the lemma for any single v.

We choose v to be the binary cubic form $x^3 - 3xy^2$. The reason for this choice is as follows. Every binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ has a naturally associated binary quadratic form, namely, the "Hessian covariant" $H_f(x, y) = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$. It is easy to see that if a binary cubic form f is acted upon by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then H_f is also acted upon by the same transformation. Now $H_v(x, y) = 9(x^2 + y^2)$, and so $\mathcal{F}H_v$ consists of the usual reduced (positive-definite) binary quadratic forms $Ax^2 + Bxy + Cy^2$, where $|B| \leq A \leq C$. Thus $\mathcal{F}v$ consists of binary cubic forms satisfying $|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd$.

Now if a binary cubic form f in $\mathcal{F}v$ has a nontrivial stabilizing element γ of order 3 in $\mathrm{SL}_2(\mathbb{Z})$, then γ will also stabilize its Hessian H_f. But the only reduced binary quadratic form, up to multiplication by scalars, having a nontrivial stabilizing element of order 3 is $x^2 + xy + y^2$. Therefore, any such C_3-type binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ in $\mathcal{F}v$ must satisfy

$$b^2 - 3ac = bc - 9ad = c^2 - 3bd.$$

From this we see that, if a, b, d are fixed, then there is at most one solution for c. As in the proof of Lemma 15, the total number of possibilities for the triple (a, b, d) in $\mathcal{F}v$ is $O(X^{3/4+\epsilon})$, and the lemma follows. $\square$

In fact, by refining the proof of Lemma 16, it can be shown that the number of C_3-points in $\mathcal{R}_X(v)$ of discriminant less than X is asymptotic to $cX^{1/2}$, where $c = \sqrt{3}/18$; see [10].

Thus, as far as Theorem 14 is concerned, the C_3-points in $V_{\mathbb{Z}}$ are negligible in number and are absorbed in the error term.

5.3 Averaging

Let $B = B(C) = \{w = (a, b, c, d) \in V : 3a^2 + b^2 + c^2 + 3d^2 \leq C, |\mathrm{Disc}(w)| \geq 1\}$; $C = 10$ will suffice in what follows. Let $V_{\mathbb{Z}}^{\mathrm{irr}}$ denote the subset of irreducible points of $V_{\mathbb{Z}}$. Then we have

$$N(V^{(i)}; X) = \frac{\int_{v \in B \cap V^{(i)}} \#\{x \in \mathcal{F}v \cap V_{\mathbb{Z}}^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\} \, |\mathrm{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv}. \tag{13}$$

The denominator of the latter expression is, by construction, a finite absolute constant greater than zero. We have chosen the measure $|\mathrm{Disc}(v)|^{-1} \, dv$ because it is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure.

More generally, for any $\mathrm{GL}_2(\mathbb{Z})$-invariant subset $S \subset V_{\mathbb{Z}}^{(i)}$, let $N(S; X)$ denote the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on S having discriminant less than X. Let S^{irr} denote the subset of irreducible points

of S. Then $N(S;X)$ can be expressed as

$$N(S;X) = \frac{\int_{v \in B \cap V^{(i)}} \#\{x \in \mathcal{F}v \cap S^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\} \, |\mathrm{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv}. \tag{14}$$

We shall use this definition of $N(S;X)$ for any $S \subset V_{\mathbb{Z}}$, even if S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant. Note that for disjoint $S_1, S_2 \subset V_{\mathbb{Z}}$, we have $N(S_1 \cup S_2) = N(S_1) + N(S_2)$.

Now since $|\mathrm{Disc}(v)|^{-1} dv$ is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure, we have for any $f \in C_0(V^{(i)})$ and $x \in V^{(i)}$ that $\int_{V^{(i)}} f(v)|\mathrm{Disc}(v)|^{-1} dv = \int_G c_i f(gx) \, dg$ for some constant c_i dependent only on whether $i = 0$ or 1; here dg denotes a left-invariant Haar measure on $G = \mathrm{GL}_2(\mathbb{R})$. We may thus express the above formula for $N(S;X)$ as an integral over $\mathcal{F} \subset \mathrm{GL}_2(\mathbb{R})$:

$$N(S;X) = \frac{1}{M_i} \int_{g \in \mathcal{F}} \#\{x \in S^{\mathrm{irr}} \cap gB : |\mathrm{Disc}(x)| < X\} \, dg \tag{15}$$

$$= \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda K} \#\{x \in S^{\mathrm{irr}} \cap n\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}\lambda k B : |\mathrm{Disc}(x)| < X\} t^{-2} dn \, d^{\times}t \, d^{\times}\lambda \, dk. \tag{16}$$

where

$$M_i = \frac{n_i}{2\pi} \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv.$$

We note that the constant 2π comes from the change of measure $|\mathrm{Disc}(v)|^{-1} dv$ to dg, as will be seen in Proposition 19. Let us write $B(n,t,\lambda,X) = n\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}\lambda B \cap \{v \in V^{(i)} : |\mathrm{Disc}(v)| < X\}$. As $KB = B$ and $\int_K dk = 1$, we have

$$N(S;X) = \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap B(n,t,\lambda,X)\} t^{-2} dn \, d^{\times}t \, d^{\times}\lambda. \tag{17}$$

To estimate the number of lattice points in $B(n,t,\lambda,X)$, we have the following two elementary propositions from the geometry-of-numbers. The first is essentially due to Davenport [13]. To state the proposition, we require the following simple definitions. A multiset $\mathcal{R} \subset \mathbb{R}^n$ is said to be *measurable* if $\mathcal{R}_k$ is measurable for all k, where $\mathcal{R}_k$ denotes the set of those points in $\mathcal{R}$ having a fixed multiplicity k. Given a measurable multiset $\mathcal{R} \subset \mathbb{R}^n$, we define its volume in the natural way, that is, $\mathrm{Vol}(\mathcal{R}) = \sum_k k \cdot \mathrm{Vol}(\mathcal{R}_k)$, where $\mathrm{Vol}(\mathcal{R}_k)$ denotes the usual Euclidean volume of $\mathcal{R}_k$.

Proposition 17 *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\bar{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implied constant in the second summand depends only on n, m, k, and ℓ.

Although Davenport states the above lemma only for compact semi-algebraic sets $\mathcal{R} \subset \mathbb{R}^n$, his proof adapts without essential change to the more general case of a bounded semi-algebraic multiset $\mathcal{R} \subset \mathbb{R}^n$, with the same estimate applying also to any image $\mathcal{R}'$ of $\mathcal{R}$ under a unipotent triangular transformation.

We now have the following lemma on the number of irreducible lattice points in $B(n,t,\lambda,X)$:

Lemma 18 *The number of lattice points (a,b,c,d) in $B(n,t,\lambda,X)$ with $a \neq 0$ is*

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < 1; \\ \mathrm{Vol}(B(n,t,\lambda,X)) + O(\max\{C^3 t^3 \lambda^3, 1\}) & \text{otherwise.} \end{cases}$$

Proof: If $C\lambda/t^3 < 1$, then $a = 0$ is the only possibility for an integral binary cubic form $ax^3 + bx^2y + cy^2 + dy^3$ in $B(n, t, \lambda, X)$, and any such binary cubic form is reducible. If $C\lambda/t^3 \geq 1$, then λ and t are positive numbers bounded from below by $(\sqrt{3}/2)^3/C$ and $\sqrt{3}/2$ respectively. In this case, one sees that the projection of $B(n, t, \lambda, X)$ onto $a = 0$ has volume $O(C^3t^3\lambda^3)$, while all other projections are also bounded by a constant times this. The lemma now follows from Proposition 17. $\square$

In (17), observe that the integrand will be nonzero only if $t^3 \leq C\lambda$ and $\lambda \leq X^{1/4}$, since B consists only of points having discriminant at least 1. Thus we may write, up to an error of $O(X^{3/4+\epsilon})$ due to Lemma 15, that

$$N(V^{(i)}; X) = \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{C^{1/3}\lambda^{1/3}} \int_{N'(t)} (\mathrm{Vol}(B(n, t, \lambda, X)) + O(\max\{C^3t^3\lambda^3, 1\}))t^{-2}\,dn\,d^{\times}t\,d^{\times}\lambda. \quad (18)$$

The integral of the first summand is

$$\frac{1}{2\pi M_i} \int_{v \in B \cap V^{(i)}} \mathrm{Vol}(\mathcal{R}_X(v))|\mathrm{Disc}(v)|^{-1}dv - \frac{1}{M_i}\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{C^{1/3}\lambda^{1/3}}^{\infty} \int_{N'(t)} \mathrm{Vol}(B(n, t, \lambda, X)t^{-2}\,dn\,d^{\times}t\,d^{\times}\lambda. \quad (19)$$

Since $\mathrm{Vol}(\mathcal{R}_X(v))$ does not depend on the choice of $v \in V^{(i)}$ (see Section 5.4), the first term of (19) is simply $\mathrm{Vol}(\mathcal{R}_X(v))/n_i$; meanwhile, the integral of the second term is easily evaluated to be $O(C^{10/3}X^{5/6}/M_i(C))$, since $\mathrm{Vol}(B(n, t, \lambda, X)) \ll C^4\lambda^4$. On the other hand, since $C^3t^3\lambda^3 \gg 1$ one immediately computes the integral of the second summand in (18) to be $O(C^{10/3}X^{5/6}/M_i(C))$. We thus obtain, for any $v \in V^{(i)}$, that

$$N(V^{(i)}; X) = \frac{1}{n_i} \cdot \mathrm{Vol}(\mathcal{R}_X(v)) + O(C^{10/3}X^{5/6}/M_i(C)). \quad (20)$$

To prove Theorem 14, it remains to compute the fundamental volume $\mathrm{Vol}(\mathcal{R}_X(v))$ for $v \in V^{(i)}$.

5.4 Computation of the fundamental volume

Define the usual subgroups K, A_+, N, and $\bar{N}$ of $\mathrm{GL}_2(\mathbb{R})$ as follows:

$$
\begin{aligned}
K &= \{\text{orthogonal transformations in } \mathrm{GL}_2(\mathbb{R})\}; \\
A_+ &= \{a(t) : t \in \mathbb{R}_+\}, \text{ where } a(t) = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}; \\
N &= \{n(u) : u \in \mathbb{R}\}, \text{ where } n(u) = \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix}; \\
\Lambda &= \left\{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}\right\} \text{ where } \lambda > 0.
\end{aligned}
$$

It is well-known that the natural product map $K \times A_+ \times N \to \mathrm{GL}_2(\mathbb{R})$ is an analytic diffeomorphism. In fact, for any $g \in \mathrm{GL}_2(\mathbb{R})$, there exist unique $k \in K$, $a = a(t) \in A_+$, and $n = n(u) \in N$ such that $g = k\,a\,n$.

Proposition 19 *For $i = 0$ or 1, let $f \in C_0(V^{(i)})$ and let x denote any element of $V^{(i)}$. Then*

$$\int_{g \in \mathrm{GL}_2(\mathbb{R})} f(g \cdot x)dg = \frac{n_i}{2\pi} \int_{v \in V^{(i)}} |\mathrm{Disc}(v)|^{-1}f(v)\,dv.$$

Proposition 19 is simply a Jacobian calculation for the change of variable from gx to v in V, where the coordinates for $g \in \mathrm{GL}_2(\mathbb{R})$ are (k, t, n, λ) with $dg = dk\,d^{\times}t\,dn\,d^{\times}\lambda$, while for v they are the usual Euclidean coordinates (a, b, c, d) with $dv = da\,db\,dc\,dd$.

It is known [22] (or readily computed using Gauss's explicit fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$) that $\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})} dg = \zeta(2)/\pi$. For a vector $v_i \in V^{(i)}$ of absolute discriminant 1, let $f : V \to \mathbb{R}$ denote the

function defined by $f(v) = |\text{Disc}(v)| \cdot m(v)$, where $m(v)$ denotes the multiplicity of v in $\mathcal{R}_X(v_i)$. Then we obtain using Proposition 19 that

$$\frac{1}{n_i} \cdot \text{Vol}(\mathcal{R}_X(v_i)) = \frac{2\pi}{n_i} \int_0^{X^{1/4}} \lambda^4 d^\times \lambda \int_{\text{GL}_2(\mathbb{Z}) \backslash \text{GL}_2^{\pm 1}(\mathbb{R})} dg = \frac{2\pi}{n_i} \cdot \frac{X}{4} \cdot \frac{\zeta(2)}{\pi} = \frac{\pi^2}{12 n_i} X,$$

where $\text{GL}_2^{\pm 1}(\mathbb{R})$ denotes the subgroup of elements in $\text{GL}_2(\mathbb{R})$ having determinant ± 1. This proves Theorem 14. Together with the Dalone-Faddeev correspondence, this also proves the main term of Theorem 4.

5.5 Congruence conditions

We may prove a version of Theorem 14 for a set in $V^{(i)}$ defined by a finite number of congruence conditions:

Theorem 20 *Suppose S is a subset of $V_{\mathbb{Z}}^{(i)}$ defined by finitely many congruence conditions. Then we have*

$$\lim_{X \to \infty} \frac{N(S \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12 n_i} \prod_p \mu_p(S), \tag{21}$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, and $n_i = 6$ or 2 for $i = 0$ or 1 respectively.

To obtain Theorem 20, suppose $S \subset V_{\mathbb{Z}}^{(i)}$ is defined by congruence conditions modulo some integer m. Then S may be viewed as the intersection of $V^{(i)}$ with the union U of (say) k translates $L_1, \ldots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice translate L_j, we may use formula (17) and the discussion following that formula to compute $N(L_j \cap V^{(i)}; X)$, where each d-dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m. With these scalings, the volumes of the d-dimensional projections of $B(n, t, \lambda, X)$, for $d = 3, 2$, and 1 are seen to be at most $O(m^{-3} C^3 t^3 \lambda^3)$, $O(m^{-2} C^2 t^4 \lambda^2)$, and $O(m^{-1} C t^3 \lambda)$ respectively. Let $a \geq 1$ be the smallest nonzero first coordinate of any point in L_j. Then, analogous to Lemma 18, the number of lattice points in $B(n, t, \lambda, X) \cap L_j$ with first coordinate nonzero is

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < a; \\ \frac{\text{Vol}(B(n, t, \lambda, X))}{m^4} + O\left(\frac{C^3 t^3 \lambda^3}{m^3} + \frac{C^2 t^4 \lambda^2}{m^2} + \frac{C t^3 \lambda}{m} + 1\right) & \text{otherwise.} \end{cases}$$

Carrying out the integral for $N(L_j; X)$ as in (18), we obtain, up to an error of $O(X^{3/4 + \epsilon})$ corresponding to the reducible points in Lemma 15, that

$$N(L_j \cap V^{(i)}; X) = \frac{\text{Vol}(\mathcal{R}_X(v))}{m^4} + O\left(\frac{1}{M_i(C)}\left[\frac{C^{10/3} X^{5/6}}{a^{1/3} m^3} + \frac{C^{8/3} X^{2/3}}{a^{2/3} m^2} + \frac{C^{4/3} X^{1/3}}{a^{1/3} m} + \log X\right]\right). \tag{22}$$

Assuming $m = O(X^{1/6})$, this gives (up to the $O(X^{3/4 + \epsilon})$ reducible points of Lemma 15):

$$N(L_j; X) = m^{-4} \text{Vol}(\mathcal{R}_X(v)) + O(m^{-3} X^{5/6}), \tag{23}$$

where the implied constant is again independent of m. Summing over j, we thus obtain

$$N(S; X) = k m^{-4} \text{Vol}(\mathcal{R}_X(v)) + O(k m^{-3} X^{5/6}) + O(X^{3/4 + \epsilon}). \tag{24}$$

Finally, the identities $k m^{-4} = \prod_p \mu_p(S)$ and $\text{Vol}(\mathcal{R}_X(v)) = \pi^2 / (12 n_i) \cdot X$ yield (21).

Note that (22)–(24) also give information on the rate of convergence of (21) for various S, which is useful in the applications; see, e.g., [1].

6 Slicing and second order terms

In Section 5, we proved that $N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + O(X^{5/6})$, where $c_1^{(0)} = \pi^2/72$ and $c_1^{(1)} = \pi^2/24$. Let $c_2^{(0)} = \sqrt{3}r/15$ and $c_2^{(1)} = r/5$ where $r = \dfrac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{\Gamma(2/3)}$. In this section, we prove that

$$N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + c_2^{(i)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}),$$

thereby proving Theorems 3 and 4.

6.1 Proofs of Theorems 3 and 4

In Equation (15) of the previous section (with $S = V_{\mathbb{Z}}^{(i)}$), we obtained a formula for the number $N(V_{\mathbb{Z}}^{(i)}; X)$ in terms of an integral over a chosen fundamental domain $\mathcal{F}$ for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$. Evaluating this integral required us to evaluate the number of integral points in $B(n, t, \lambda, X)$ for various n, t, λ, X. Using Proposition 17, we concluded that the number of integral points in $B(n, t, \lambda, X)$ is equal to the volume of $B(n, t, \lambda, X)$ with an error of $O(t^3 \lambda^3)$.

In this section, we count points in dyadic ranges of the discriminant. Let $B(n, t, \lambda, X/2, X)$ be the subset of $B(n, t, \lambda, X)$ that contains points having discriminant greater than $X/2$. We again estimate the number of integer points in $B(n, t, \lambda, X/2, X)$ to be equal to its volume, again with an error of $O(t^3 \lambda^3)$. To obtain a more precise count for the number of lattice points in $B(n, t, \lambda, X/2, X)$ when t is large, we *slice* the set $B(n, t, \lambda, X/2, X)$ by the coefficient of x^3. More precisely, for $a \in \mathbb{Z}$, let $B_a(n, t, \lambda, X/2, X)$ denote the set of binary cubic forms in $B(n, t, \lambda, X/2, X)$ whose x^3 coefficient is equal to a. Then we have:

$$\#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} = \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B_a(n, t, \lambda, X/2, X)\}. \tag{25}$$

We then again use Proposition 17 to estimate the right hand side of (25). We shall slice the set $B(n, t, \lambda, X/2, X)$ when t is "large". We separate the large t from the small as follows:

Let Ψ be a smooth function on $\mathbb{R}_{\geq 0}$ such that $\Psi(x) = 1$ for $x \leq 2$ and $\Psi(x) = 0$ for $x \geq 3$. Let Ψ_0 denote the function $1 - \Psi$. Let $N(V_{\mathbb{Z}}^{(i)}; X/2, X)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i),\mathrm{irr}}$ having discriminant between $X/2$ and X. Then for any $\kappa > 0$, we have just as in (17) that

$$
\begin{aligned}
N(V_{\mathbb{Z}}^{(i)}; X/2, X) \;=\; & \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn \, d^\times t \, d^\times \lambda \\
& + \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn \, d^\times t \, d^\times \lambda.
\end{aligned}
\tag{26}
$$

Note that the first summand of the right hand side of (26) is non-zero only when $t < 3\lambda^{1/3}/\kappa$, while the second summand is non-zero only when $t > 2\lambda^{1/3}/\kappa$. We will choose κ later to minimize our error term.

As the absolute value of the discriminant of every point in B is bounded below by 1, we see that $B(n, t, \lambda, X/2, X)$ is empty when $\lambda > X^{1/4}$. Thus, from Proposition 17, we see that the first summand of the right hand side of (26) is

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) (\mathrm{Vol}(B(n, t, \lambda, X/2, X)) + O(\max\{t^3\lambda^3, 1\})) t^{-2} dn d^\times t d^\times \lambda. \tag{27}$$

The integral of the error term in the integrand of (27) is easily seen to be

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \lambda^3 t \, d^\times t \, d^\times \lambda\right) = O\left(\frac{X^{5/6}}{\kappa}\right).$$

13

Therefore, the first summand of the right hand side of (26) is equal to

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t d^\times \lambda + O\left(\frac{X^{5/6}}{\kappa}\right), \qquad (28)$$

where $B(x,y)$ denotes the set of all points in B with discriminant between x and y.

To evaluate the second summand on the right hand side of (26), we break up the integrand into a sum over points with fixed x^3 coefficient. Indeed, we see that it is equal to

$$\frac{1}{M_i} \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \int_{\mathcal{F}} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B_a(n, t, \lambda, X/2, X)\} dg. \qquad (29)$$

As B is K-invariant, the number of points in $B_a(n,t,\lambda,X/2,X)$ is equal to the number of points in $B_{-a}(n,t,\lambda,X/2,X)$. Note that the integrand vanishes for $a > O(\kappa^3)$ where the implied constant depends only on B. We again use Proposition 17 to see that (29) is equal to

$$\frac{2}{M_i} \sum_{a=1}^{O(\kappa^3)} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) (\mathrm{Vol}(B_a(n,t,\lambda,X/2,X)) + O(\max\{\lambda^2 t^4, 1\})) t^{-2} dn d^\times t d^\times \lambda. \qquad (30)$$

Again, we can estimate the integral of the error in (30) to be of the order of

$$\sum_{a=1}^{O(\kappa^3)} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/a^{1/3}} \lambda^2 t^4 \, t^{-2} d^\times t \, d^\times \lambda = X^{2/3} \sum_{a=1}^{O(\kappa^3)} O(a^{-2/3}) = O\left(\kappa X^{2/3}\right).$$

We assume from now on that $\kappa \leq X^{1/12}$. It follows that if $\Psi_0(t\kappa/\lambda^{1/3})$ is nonzero, then $t > 1$ and thus the integral over N' in (30) always goes between $-1/2$ and $1/2$. The integral of the main term in (30) is now computed to be

$$\frac{2}{M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) (\mathrm{Vol}(B_a(0, t, \lambda, X/2, X))) t^{-2} d^\times t d^\times \lambda$$

$$= \frac{2}{M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^3 t^3 \mathrm{Vol}(B_{\frac{at^3}{\lambda}}(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t d^\times \lambda, \qquad (31)$$

where $B_a(x,y)$ denotes the set of forms in B having their x^3 coordinate equal to a and discriminant between x and y. We change variables to compute the right hand side of (31); let $u = \frac{t^3 a}{\lambda}$ so that $d^\times u = 3 d^\times t$. The main term in (30) is therefore equal to

$$\frac{2}{3M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) \frac{\lambda^{10/3} u^{1/3}}{a^{1/3}} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u d^\times \lambda. \qquad (32)$$

To compute the expression above, we first sum over a. Let $\Phi(z)$ be equal to $\Psi_0(u^{1/3}/z^{1/3})$. Let $\widetilde{\Phi}$ and $\widetilde{\Psi}$ denote the Mellin transforms of Φ and Ψ respectively. Since Ψ_0 is smooth and Schwartz class, the Mellin transforms $\tilde{\Phi}(s)$ and $\tilde{\Psi}_0(s)$ are rapidly decaying on any vertical line $\sigma + it$ as $|t| \to \infty$. Therefore,

$$\sum_{a=1}^{\infty} a^{-\frac{1}{3}} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) = \int_{\mathrm{Re}\ s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Phi}(s) \kappa^{3s} ds \qquad (33)$$

$$= 3 \int_{\mathrm{Re}\ s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Psi}_0(-3s)(\kappa^3 u)^s ds \qquad (34)$$

$$= \zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2)(\kappa^3 u)^{2/3} + O(\min\{(\kappa^3 u)^{-M}, 1\}), \qquad (35)$$

14

for any integer M, where we obtain the last equality by moving the line of integration to Re $s = -M$. Therefore, (32) is equal to

$$\frac{2}{3M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \left[\zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2)(\kappa^3 u)^{2/3} \right] \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda, \quad (36)$$

with an error of

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \min\{(\kappa^3 u)^{-M}, 1\} \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda, \right). \quad (37)$$

We shall eventually choose κ to be equal to $X^{1/12}$. Therefore, (37) can be bounded above by

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u=0}^{X^{\epsilon-1/4}} \lambda^{10/3} u^{1/3} d^\times u \, d^\times \lambda \right) = O_\epsilon(X^{3/4+\epsilon}). \quad (38)$$

We now evaluate the integral of the two summands in the integrand of (36) separately. Evaluating the integral of the second summand, we obtain

$$\frac{2}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \widetilde{\Psi}_0(-2)\kappa^2 \lambda^{10/3} u \, \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda \quad (39)$$

$$= \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \widetilde{\Psi}_0(-2)\kappa^2 \lambda^{10/3} \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) d^\times \lambda, \quad (40)$$

which is simply equal to

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=0}^{\infty} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^{\frac{10}{3}+\frac{2}{3}} \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda. \quad (41)$$

Adding (41) to the main term of (28) gives us the following.

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \left(\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) + \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda$$

$$= \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} (\mathrm{Vol}(B(n, t, \lambda, X/2, X))) t^{-2} d^\times t \, d^\times \lambda,$$

which can be evaluated, as in Section 5, to be equal to $c_1^{(i)} X/2$.

Now the first summand in (36) is

$$\frac{2}{3M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \zeta\left(\frac{1}{3}\right) \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda. \quad (42)$$

Let $a(v), b(v), c(v)$, and $d(v)$ denote the four coordinates of points $v \in B$. Then (42) is equal to

$$\frac{1}{3M_i} \zeta\left(\frac{1}{3}\right) \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{B(X/(2\lambda^4), X/\lambda^4)} \lambda^{10/3} a(v)^{1/3} \frac{dv}{a(v)} d^\times \lambda$$

$$= \frac{1}{3M_i} \zeta\left(\frac{1}{3}\right) \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{B(X/(2\lambda^4), X/\lambda^4)} \lambda^{10/3} a(v)^{-2/3} dv \, d^\times \lambda.$$

Carrying out the integral over λ in the right hand side of the above equation, we see that (42) is equal to

$$\frac{1}{10M_i} \zeta\left(\frac{1}{3}\right) \left(1 - \frac{1}{2^{5/6}}\right) X^{5/6} \int_B |\mathrm{Disc}(v)|^{-5/6} a(v)^{-2/3} dv. \quad (43)$$

15

Recalling the definition of M_i, we see that (42) is equal to

$$\frac{2\pi}{10n_i}\zeta\left(\frac{1}{3}\right)\left(1-\frac{1}{2^{5/6}}\right)X^{5/6}\frac{\int_B |\text{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B |\text{Disc}(v)|^{-1}dv}.$$

We now evaluate the ratio

$$\frac{\int_B |\text{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B |\text{Disc}(v)|^{-1}dv}. \tag{44}$$

The ratio in (44) is independent of the K-invariant set B. Thus, for any $f \in V_\mathbb{R}^{(i)}$, (44) is equal to

$$|\text{Disc}(f)|^{1/6}\int_K a(\gamma \cdot f)^{-2/3}d\gamma = |\text{Disc}(f)|^{1/6}\int_K f((1,0)\cdot\gamma)^{-2/3}d\gamma = \frac{|\text{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi}f(\cos(\theta),\sin(\theta))^{-2/3}d\theta.$$

We now choose convenient points $f \in V_\mathbb{R}^{(i)}$ for $i = 0, 1$. For $i = 1$ we choose $f(x,y) = x^3 + xy^2$ which has discriminant -4. Then

$$\frac{|\text{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi}f(\cos(\theta),\sin(\theta))^{-2/3}d\theta = \frac{2^{1/3}}{2\pi}\int_0^{2\pi}\cos(\theta)^{-2/3}d\theta = \frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos(\theta)^{-2/3}d\theta.$$

The substitution $y = \cos(\theta)$ yields

$$\frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos(\theta)^{-2/3}d\theta = \frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy.$$

The substitution $z = y^2$ then gives

$$\frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy = \frac{2^{1/3}}{\pi}\int_0^1 z^{-5/6}(1-z)^{-1/2}dz = \frac{2^{1/3}\Gamma(1/6)\Gamma(1/2)}{\pi\Gamma(2/3)},$$

where the final equality follows from evaluating the beta function $B(\frac{1}{2}, \frac{1}{6})$. Using the standard identities

$$\begin{aligned}
\Gamma(1/6) &= 2^{5/3}3^{-1/2}\pi^{3/2}/\Gamma(2/3)^2, \\
\Gamma(2/3) &= 3^{-1/2}2\pi/\Gamma(1/3), \\
\zeta(1/3) &= (2\pi)^{-2/3}\Gamma(2/3)\zeta(2/3),
\end{aligned} \tag{45}$$

we finally see that (43) is equal to $\left(1 - \frac{1}{2^{5/6}}\right)c_2^{(1)}X^{5/6}$.

Similarly, for $i = 0$ we choose the form $f(x,y) = x^3 - 3xy^2 \in V_\mathbb{R}^{(0)}$. Using the identity $\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)$ we see, exactly as above, that (43) is equal to $\left(1 - \frac{1}{2^{5/6}}\right)c_2^{(0)}X^{5/6}$. Therefore, we have

$$N(V_\mathbb{Z}^{(i)}; X/2, X) = c_1^{(i)}X/2 + c_2^{(i)}(1 - 1/2^{5/6})X^{5/6} + O(X^{2/3}\kappa) + O(X^{5/6}/\kappa),$$

and choosing κ to be equal to $X^{1/12}$ proves Theorems 3 and 4.

6.2   Congruence conditions

Let $S \subset V_\mathbb{Z}^{(i)}$ be a $GL_2(\mathbb{Z})$-invariant set. We define $N(S; X/2, X)$ to be the number of irreducible $GL_2(\mathbb{Z})$-orbits on S having discriminant between $X/2$ and X. Identically as in (26), we then have

$$\begin{aligned}
N(S; X/2, X) &= \frac{1}{M_i}\int_{N'(a)A'\Lambda}\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\{x \in S^{\text{irr}} \cap B(n,t,\lambda,X/2,X)\}t^{-2}dn\,d^\times t\,d^\times\lambda \\
&\quad + \frac{1}{M_i}\int_{N'(a)A'\Lambda}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\{x \in S^{\text{irr}} \cap B(n,t,\lambda,X/2,X)\}t^{-2}dn\,d^\times t\,d^\times\lambda.
\end{aligned}$$

We shall use this definition of $N(S; X/2, X)$ even when the set S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant.

Suppose $\mathcal{L} \subset V_{\mathbb{Z}}$ is any sublattice of index m in $V_{\mathbb{Z}}$. In what follows, we compute the value $N(\mathcal{L} \cap V^{(i)}; X)$, for $i = 0, 1$. The computation is very similar to the computation of $N(V_{\mathbb{Z}}^{(i)}; X)$ and we highlight the differences that occur.

We have

$$
\begin{aligned}
N(\mathcal{L} \cap V^{(i)}; X/2, X) &= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^{\times}t\, d^{\times}\lambda \\
&+ \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^{\times}t\, d^{\times}\lambda.
\end{aligned}
\tag{46}
$$

As in (28), we see that the first summand of the right hand side of (46) is equal to

$$
\frac{1}{mM_i} \int_{\lambda = (\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^{\times}t d^{\times}\lambda + O\left(\frac{X^{5/6}}{\kappa}\right),
\tag{47}
$$

and as in (29), we see that the second summand of the right hand side of (46) is equal to

$$
\frac{1}{M_i} \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \int_{\mathcal{F}} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L}^{\mathrm{irr}} \cap V^{(i)} \cap B_a(n, t, \lambda; X/2, X)\} dg.
\tag{48}
$$

We can write $m = m_1 m_2$ such that the coefficient of x^3 of every element in $\mathcal{L}$ is a multiple of m_1 and the index of $\mathcal{L}_a$ in V_a is equal to m_2, where $\mathcal{L}_a$ is the set of all forms in $\mathcal{L}$ whose x^3 coefficient is equal to a. As in (32), we estimate (48) to be

$$
\frac{2}{3m_2 M_i} \sum_{\substack{a=1 \\ m_1 | a}}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) \frac{\lambda^{10/3} u^{1/3}}{a^{1/3}} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^{\times}u d^{\times}\lambda + O(\kappa X^{2/3}).
\tag{49}
$$

Analogously to our computations from (33) to (36), we have

$$
\sum_{\substack{a=1 \\ m_1 | a}}^{\infty} a^{-\frac{1}{3}} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) = m_1^{-1/3} \int_{\mathrm{Re}\, s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Phi}(s)(m_1^{-1/3}\kappa)^{3s} ds
\tag{50}
$$

$$
= 3 m_1^{-1/3} \int_{\mathrm{Re}\, s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Psi}_0(-3s)((m_1^{-1/3}\kappa)^3 u)^s ds
\tag{51}
$$

$$
= m_1^{-1/3} \zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2) m_1^{-1}(\kappa^3 u)^{2/3} + O(\min\{(m_1^{-1}\kappa^3 u)^{-M}, 1\}),
\tag{52}
$$

for any integer M.

Identically as in (38), if we choose κ to be equal to $X^{1/12}$, then the error coming from the term $O(\min\{(m_1^{-1}\kappa^3 u)^{-M}, 1\})$ is equal to $O_{\epsilon}(m_1^{1/3} X^{3/4+\epsilon})$. We thus have the following theorem.

Theorem 21 *Let $\mathcal{L} \subset V_{\mathbb{Z}}$ be a sublattice of index m in $V_{\mathbb{Z}}$. Write $m = m_1 m_2$, where the coefficient of x^3 of elements in $\mathcal{L}$ is a multiple of m_1 and the corresponding index of $\mathcal{L}_a$ in V_a is equal to m_2. Then*

$$
N(\mathcal{L} \cap V^{(i)}; X/2, X) = \frac{c_1^{(i)}}{m} \frac{X}{2} + \left(1 - \frac{1}{2^{5/6}}\right) \frac{c_2^{(i)}}{m_1^{1/3} m_2} X^{5/6} + O_{\epsilon}(m_1^{1/3} X^{3/4+\epsilon}).
\tag{53}
$$

Summing over the dyadic ranges of the discriminant, we also then obtain

$$
N(\mathcal{L} \cap V^{(i)}; X) = \frac{c_1^{(i)}}{m} X + \frac{c_2^{(i)}}{m_1^{1/3} m_2} X^{5/6} + O_{\epsilon}(m_1^{1/3} X^{3/4+\epsilon}).
\tag{54}
$$

17

7 p-adic densities for the second term

Let p be a fixed prime and σ be the splitting type (f, p) at p of an integral binary cubic form f. The methods of the previous section allow us to count the asymptotic number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $\mathcal{U}_p(\sigma)$ having bounded discriminant.

More precisely, let us define $\mu_1(\sigma, p)$, $\mu_2(\sigma, p)$, $\mu_1(p)$, and $\mu_2(p)$ so that

$$
\begin{aligned}
N(\mathcal{U}_p(\sigma) \cap V^{(i)}; X) &= \mu_1(\sigma, p)c_1^{(i)} X + \mu_2(\sigma, p)c_2^{(i)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
N(\mathcal{U}_p; X) &= \mu_1(p)c_1^{(i)} X + \mu_2(p)c_2^{(i)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
$$

The values of $\mu_1(\sigma, p)$ and $\mu_1(p)$ were computed in Section 4 to be equal to $\mu(\mathcal{U}_p(\sigma))$ and $\mu(\mathcal{U}_p)$, respectively. In this section we compute the values of $\mu_2(\sigma, p)$ and $\mu_2(p)$ for all splitting types σ and all primes p. We will require these results to prove Theorem 2.

From the results of Section 4, we see that $\mathcal{U}_p(111) = T_p(111)$, $\mathcal{U}_p(12) = T_p(12)$, and $\mathcal{U}_p(3) = T_p(3)$. For $\sigma = (111), (12), (3)$, we write $T_p(\sigma)$ as a union of lattices in the following way. Let α, β, γ be distinct elements in $\mathbb{P}^1_{\mathbb{F}_p}$. Let $T_p(\alpha, \beta, \gamma)$ be the set of all elements $f \in V_{\mathbb{Z}}$ such that the reduction of f modulo p has roots α, β, and γ. Then

$$
\begin{aligned}
T_p(111) &= \bigcup_{\alpha, \beta, \gamma \,\in\, \mathbb{P}^1_{\mathbb{F}_p}} (T_p(\alpha, \beta, \gamma) \setminus p \cdot V_{\mathbb{Z}}), \\
T_p(12) &= \bigcup_{\alpha \in \mathbb{P}^1_{\mathbb{F}_p}, \,\beta_1, \beta_2 \in \mathbb{P}^1_{\mathbb{F}_{p^2}}} (T_p(\alpha, \beta_1, \beta_2) \setminus p \cdot V_{\mathbb{Z}}), \\
T_p(3) &= \bigcup_{\gamma_1, \gamma_2, \gamma_3 \,\in\, \mathbb{P}^1_{\mathbb{F}_{p^3}}} (T_p(\gamma_1, \gamma_2, \gamma_3) \setminus p \cdot V_{\mathbb{Z}}),
\end{aligned}
$$

where β_1, β_2 are $\mathbb{F}_p$-conjugate points in $\mathbb{F}_{p^2}$ and $\gamma_1, \gamma_2, \gamma_3$ are $\mathbb{F}_p$-conjugate points in $\mathbb{F}_{p^3}$.

Similarly, the set $T_p(1^2 1)$ (resp. $T_p(1^3)$) can be written as the union over pairs of distinct points $\alpha, \beta \in \mathbb{F}_p$ (resp. points $\alpha \in \mathbb{F}_p$) of the sets $T_p(1^2 1, \alpha, \beta)$ (resp. $T_p(1^3, \alpha)$) which consist of elements $f \in V_{\mathbb{Z}}$ whose reduction modulo p has a double root at α and a single root at β (resp. a triple root at α). Furthermore, the results of Section 4 imply that elements f in $T_p(1^2 1, \alpha, \beta)$ or $T_p(1^3, \alpha)$ correspond to rings that are non-maximal at p if and only if $f(\tilde{\alpha})$ is a multiple of p^2, where $\tilde{\alpha}$ is any element in $\mathbb{Z}$ whose reduction modulo p is equal to α.

We can now compute the values of $\mu_2(\sigma, p)$ from Theorem 21. Let $\sigma = (111)$. We apply Theorem 21 to the lattices $T_p(\alpha, \beta, \gamma)$ and $p \cdot V_{\mathbb{Z}}$. For the lattice $T_p([1 : 0], \beta, \gamma)$ we have $m_1 = p$ and $m_2 = p^2$ in the notation of Theorem 21. Therefore

$$
N(T_p([1 : 0], \beta, \gamma); X) = \frac{c_1^{(i)}}{p^3} X + \frac{c_2^{(i)}}{p^{7/3}} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

For the lattice $T_p(\alpha, \beta, \gamma)$, where none of α, β, and γ are equal to $[1 : 0] \in \mathbb{P}^1_{\mathbb{F}_p}$, we have $m_1 = 1$ and $m_2 = p^3$. Therefore

$$
N(T_p(\alpha, \beta, \gamma); X) = \frac{c_1^{(i)}}{p^3} X + \frac{c_2^{(i)}}{p^3} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

Finally for the lattice $p \cdot V_{\mathbb{Z}}$ we have $m_1 = p$ and $m_2 = p^3$. Therefore,

$$
N(p \cdot V_{\mathbb{Z}}; X) = \frac{c_1^{(i)}}{p^4} X + \frac{c_2^{(i)}}{p^{10/3}} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

There are $\binom{p}{2}$ lattices $T_p([1 : 0], \beta, \gamma)$ and $\binom{p}{3}$ lattices $T_p(\alpha, \beta, \gamma)$ where none of α, β, and γ are equal to $[1 : 0]$. Thus we have

$$
\mu_2((111), p) = p^{-3}\left(\binom{p}{2}(p-1)p^{-1/3} + \binom{p}{3}(1 - p^{-1/3}) \right).
$$

18

σ	$\mu_1(\sigma, p)$	$\mu_2(\sigma, p)$
(111)	$\frac{1}{6}(p-1)^2 \, p \, (p+1) \, / \, p^4$	$p^{-3}\left(\binom{p}{3}(1-p^{-1/3}) + \frac{p(p-1)}{2}(p-1)p^{-1/3}\right)$
(12)	$\frac{1}{2}(p-1)^2 \, p \, (p+1) \, / \, p^4$	$p^{-3}\left(p\left(\frac{p^2-p}{2}\right)(1-p^{-1/3}) + \frac{p^2-p}{2}(p-1)p^{-1/3}\right)$
(3)	$\frac{1}{3}(p-1)^2 \, p \, (p+1) \, / \, p^4$	$p^{-3}\left(\left(\frac{p^3-p}{3}\right)(1-p^{-1/3})\right)$
$(1^2 1)$	$(p-1)^2 \, (p+1) \, / \, p^4$	$p^{-3}\left(p(p-1)\left(1-\frac{1}{p}\right) + p(p-1)(1-p^{-1/3})p^{-1/3}\right)$
(1^3)	$(p-1)^2 \, (p+1) \, / \, p^5$	$p^{-3}\left(p(1-p^{-1/3})\left(1-\frac{1}{p}\right) + (p-1)(1-p^{-1/3})p^{-1/3}\right)$

Table 1: Values of p-adic densities for splitting types

Computations for the other values of σ are similar and we list the results in Table 1.

Adding up the values of the $\mu_1(\sigma, p)$ and the $\mu_2(\sigma, p)$, we obtain the following lemma.

Lemma 22 *We have:*

$$
\begin{aligned}
\mu_1(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^3}\right), \\
\mu_2(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^{5/3}}\right).
\end{aligned}
\tag{55}
$$

8 Proofs of the main terms of Theorems 1–6

In this section, we use the results of Sections 1–5 to complete the proofs of the main terms of Theorems 1–6 and Corollary 7.

We have already proven the main term (indeed even the second main term) of Theorems 3 and 4, which give counts for the number of isomorphism classes of integral binary cubic forms and cubic orders, respectively, having bounded discriminant. In fact, Theorem 20 gives the analogous count of integral binary cubic forms satisfying any specified finite set of congruence conditions.

We recall from Section 3, however, that the set S of elements in $V_{\mathbb{Z}}$ corresponding to maximal orders is defined by infinitely many congruence conditions. Similarly, we show in Section 8.1 that the count in Corollary 7 of 3-torsion elements in class groups of quadratic fields is equal to the count of integer binary cubic forms in another set S that too is defined by infinitely many congruence conditions. To prove that (21) still holds for such sets S, we require a uniform estimate on the error term when only finitely many factors are taken in (21). This uniformity estimate is proven in Section 8.2.

In Sections 8.3, 8.4, and 8.5, we then carry out a sieve, using this uniformity estimate, to prove the main terms of Theorems 1–2, 5–6, and Corollary 7, respectively.

8.1 Cubic fields with no totally ramified primes

To prove Corollary 7, we consider those cubic fields in which no prime is totally ramified. The significance of being "nowhere totally ramified" is as follows. Given an S_3-cubic field K_3, let K_6 denote its Galois closure. Let K_2 denote a quadratic field contained in K_6 (the "quadratic resolvent field"). Then one checks that the Galois cubic extension K_6/K_2 is unramified precisely when the cubic field K_3 is nowhere totally ramified. Conversely, if K_2 is a quadratic field, and K_6 is any unramified cubic extension of K_2, then as an extension of the base field $\mathbb{Q}$, the field K_6 is Galois with Galois group S_3, and any cubic subfield K_3 of K_6 is then nowhere totally ramified.

8.2 A uniformity estimate

As in Section 4, let us denote by $\mathcal{V}_p$ the set of all $f \in V_{\mathbb{Z}}$ corresponding to cubic rings R that are maximal at p and in which p is not totally ramified. Furthermore, let $\mathcal{Z}_p = V_{\mathbb{Z}} - \mathcal{V}_p$ (thus $\mathcal{Z}_p$ consists of those binary cubic forms whose discriminants are not fundamental). In order to apply a simple sieve to obtain the main terms of Theorems 1, 2, 5, 6 and Corollary 7, we require the following proposition:

Proposition 23 $N(\mathcal{Z}_p; X) = O(X/p^2)$, where the implied constant is independent of p.

Proof: The set $\mathcal{Z}_p$ may be naturally partitioned into two subsets: $\mathcal{W}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings not maximal at p; and $\mathcal{Y}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings that are maximal at p but also totally ramified at p.

　　We first treat $\mathcal{W}_p$. Recall that the *content* $\mathrm{ct}(R)$ of a cubic ring R is defined as the maximal integer n such that $R = \mathbb{Z} + nR'$ for some cubic ring R'. It follows from (7) that the content of R is simply the content (i.e., the greatest common divisor of the coefficients) of the corresponding binary cubic form f. We say R is *primitive* if $\mathrm{ct}(R) = 1$, and R is *primitive at p* if $\mathrm{ct}(R)$ is not a multiple of p.

Lemma 24 *Suppose R is a cubic ring that is primitive at p. Then the number of subrings of index p in R is at most* 3.

Proof: Suppose R has multiplication table (7) in terms of a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ for R, and let $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be the corresponding binary cubic form. Then it is clear from (7) that the $\mathbb{Z}$-module spanned by $1, p \cdot \omega, \theta$ forms a ring if and only if $d = 0$, i.e., if $(0, 1)$ is a root of the cubic form f. Since R is primitive at p, the form f is nonzero (mod p) and hence has at most three distinct roots in $\mathbb{P}^1_{\mathbb{F}_p}$. It follows that R can have at most three subrings of index p. $\square$

　　To prove the proposition, suppose R is a cubic ring of absolute discriminant less than X that is not maximal at p. By Lemma 9, R has a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ such that either (i) $R' = \mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ forms a cubic ring, or (ii) $R'' = \mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ forms a cubic ring.

　　Assume we are in case (i), i.e., R' is a ring. If R' is primitive at p, then we have that $\mathrm{Disc}(R') = \mathrm{Disc}(R)/p^2 < X/p^2$; thus the total number of possible rings R' that can arise is $O(X/p^2)$ by Theorem 4. By Lemma 24, the number of R that can correspond to such R' is at most three times that, which is also $O(X/p^2)$. On the other hand, if R' is not primitive at p, then let S be the ring such that $R' = \mathbb{Z} + pS$. Then $\mathrm{Disc}(S) < \mathrm{Disc}(R)/p^6 < X/p^6$, so the number of possibilities for S is $O(X/p^6)$, which is thus the number of possibilities for R' (since $R' = \mathbb{Z} + pS$). The number of possibilities for R is then $p + 1$ (the number of index p submodules of a rank 2 $\mathbb{Z}$-module) times the number of possibilities for R', yielding $O((p+1)X/p^6)$ possibilites. We conclude that in case (i), the number of possibilities for R is $O(X/p^2) + O((p+1)X/p^6) = O(X/p^2)$.

　　Assume we are now in case (ii), i.e., R'' is a ring. Then $R = \mathbb{Z} + pR''$ where $\mathrm{Disc}(R'') = \mathrm{Disc}(R)/p^4 < X/p^4$. The number of possible R'' in this case is $O(X/p^4)$ by Theorem 4, and thus the number of possible cubic rings $R = \mathbb{Z} + pR''$ arising from case (ii) is $O(X/p^4)$. Thus the total number $N(\mathcal{W}_p; X)$ of cubic rings R that are not maximal at p and have absolute discriminant less than X is $O(X/p^2) + O(X/p^4) = O(X/p^2)$, as desired.

　　Finally, that $N(\mathcal{Y}_p; X) = O(X/p^2)$ follows easily from class field theory. A nice, short exposition of this may be found in, e.g., [12, p. 15]. $\square$

8.3 Density of discriminants of cubic fields (Proof of Theorem 1)

We may now prove the main terms of Theorems 1 and 2. Let $\mathcal{U} = \cap_p \mathcal{U}_p$. Then $\mathcal{U}$ is the set of $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings R. By Lemma 13, the p-adic density of $\mathcal{U}_p$ is given by $\mu(\mathcal{U}_p) = (1 - p^{-2})(1 - p^{-3})$. Suppose Y is any positive integer. It follows from (21) that

$$\lim_{X \to \infty} \frac{N(\cap_{p<Y} \mathcal{U}_p \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12n_i} \prod_{p<Y} [(1 - p^{-2})(1 - p^{-3})].$$

Letting Y tend to ∞, we obtain immediately that

$$\limsup_{X\to\infty} \frac{N(\mathcal{U}\cap V^{(i)};X)}{X} \le \frac{\pi^2}{12n_i}\prod_p[(1-p^{-2})(1-p^{-3})] = \frac{1}{2n_i\zeta(3)}.$$

To obtain a lower bound for $N(\mathcal{U}\cap V^{(i)};X)$, we note that

$$\bigcap_{p<Y}\mathcal{U}_p \subset (\mathcal{U}\cup\bigcup_{p\ge Y}\mathcal{W}_p).$$

Hence by Proposition 23,

$$\lim_{X\to\infty} \frac{N(\mathcal{U}\cap V^{(i)};X)}{X} \ge \frac{\pi^2}{12n_i}\prod_{p<Y}[(1-p^{-2})(1-p^{-3})] - O(\sum_{p\ge Y}p^{-2}).$$

Letting Y tend to infinity completes the proof.

We note that the same arguments also apply when counting cubic fields with specified local behavior at finitely many primes.

8.4 A simultaneous generalization (Proof of Theorem 6)

We now prove the main terms of Theorems 5 and 6, which give the density of discriminants of cubic orders or fields satisfying any finite number (or in many natural cases, an infinite number) of local conditions. Towards this end, for each prime p let Σ_p be a set of isomorphism classes of nondegenerate cubic rings over $\mathbb{Z}_p$. (By *nondegenerate*, we mean having nonzero discriminant over $\mathbb{Z}_p$, so that it can arise as $R\otimes\mathbb{Z}_p$ for some cubic order R over $\mathbb{Z}$.) We denote the collection (Σ_p) of these local specifications over all primes p by Σ. We say that the collection $\Sigma = (\Sigma_p)$ is *acceptable* if, for all sufficiently large p, the set Σ_p contains at least the maximal cubic rings over $\mathbb{Z}_p$ that are not totally ramified at p.

For a cubic order R over $\mathbb{Z}$, we write "$R\in\Sigma$" (or say that "R is a Σ-order") if $R\otimes\mathbb{Z}_p\in\Sigma_p$ for all p. We wish to determine the number of Σ-orders R of bounded discriminant, for any acceptable collection Σ of local specifications.

To this end, fix an acceptable $\Sigma = (\Sigma_p)$ of local specifications, and also fix any $i\in\{0,1\}$. Let $S = S(\Sigma, i)$ denote the set of all irreducible $f\in V_{\mathbb{Z}}^{(i)}$ such that the corresponding cubic ring $R(f)\in\Sigma$. Then the number of Σ-orders with discriminant at most X is given by $N(S;X)$. We prove the following asymptotics for $N(S;X)$.

Theorem 25 *We have* $\displaystyle\lim_{X\to\infty} \frac{N(S(\Sigma,i);X)}{X} = \frac{1}{2n_i}\prod_p\Big(\frac{p-1}{p}\cdot\sum_{R\in\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|}\Big).$

Although $S = S(\Sigma, i)$ might again be defined by infinitely many congruence conditions, the estimate provided in Proposition 23 (and the fact that Σ is acceptable) shows that equation (21) continues to hold for the set S; the argument is identical to that in the proof of Theorem 1.

We now evaluate $\mu_p(S)$ in terms of the cubic rings lying in Σ_p.

Lemma 26 *We have*
$$\mu_p(S(\Sigma,i)) = \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4}\cdot\sum_{R\in\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|}.$$

Proof: The proof of Theorem 1, with $\mathbb{Z}_p$ in place of $\mathbb{Z}$, shows that for any cubic $\mathbb{Z}_p$-algebra R there is a unique element $v\in V_{\mathbb{Z}_p}$ up to $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence satisfying $R_{\mathbb{Z}_p}(f) = R$. Moreover, the automorphism group of such a cubic $\mathbb{Z}_p$-algebra R is simply the size of the stabilizer in $\mathrm{GL}_2(\mathbb{Z}_p)$ of the corresponding element $v\in V_{\mathbb{Z}_p}$.

We normalize Haar measure dg on the p-adic group $\mathrm{GL}_2(\mathbb{Z}_p)$ so that $\int_{g \in \mathrm{GL}_2(\mathbb{Z}_p)} dg = \#\mathrm{GL}_2(\mathbb{F}_p)$. Since $|\mathrm{Disc}(x)|_p^{-1} \cdot dx$ is a $\mathrm{GL}_2(\mathbb{Q}_p)$-invariant measure on $V_{\mathbb{Z}_p}$, we must have for any cubic $\mathbb{Z}_p$-algebra $R = R(v_0)$ that

$$\int_{\substack{x \in V_{\mathbb{Z}_p} \\ R(x)=R}} dx = c \cdot \int_{g \in \mathrm{GL}_2(\mathbb{Z}_p)/\mathrm{Stab}(v_0)} |\mathrm{Disc}(gv_0)|_p \cdot dg = c \cdot \frac{|\mathrm{Disc}(R)|_p \cdot \#\mathrm{GL}_2(\mathbb{F}_p)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(R)},$$

for some constant c. A Jacobian calculation using an indeterminate v_0 satisfying $\mathrm{Disc}(v_0) \neq 0$ shows that $c = p^{-4}$, independent of v_0. The lemma follows. $\square$

Finally, we observe that $\#\mathrm{GL}_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$, and so

$$\frac{\pi^2}{12n_i} \prod_p \mu_p(S(\Sigma, i)) = \frac{\pi^2}{12n_i} \prod_p \left(1 - \frac{1}{p^2}\right)\left(\frac{p-1}{p}\right) \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|},$$

proving Theorem 25. Noting that $n_1 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^3)$ and $n_2 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C})$ also then yields Theorem 6.

Remark. Lemma 26, together with the identities $\mu_p(V_{\mathbb{Z}_p}) = 1$ and $\mu_p(\mathcal{U}_p) = (p^3-1)(p^2-1)/p^5$ of Lemma 13, give the interesting formulae

$$\sum_{R \text{ cubic ring } / \mathbb{Z}_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} = \left(1 - \frac{1}{p}\right)^{-1}\left(1 - \frac{1}{p^2}\right)^{-1} \tag{56}$$

and

$$\sum_{K \text{ etale cubic extension of } \mathbb{Q}_p} \frac{1}{\mathrm{Disc}_p(K)} \cdot \frac{1}{|\mathrm{Aut}(K)|} = 1 + \frac{1}{p} + \frac{1}{p^2}. \tag{57}$$

(Note that (56) is an infinite sum!) What is remarkable about these formulae is that their statements are independent of p. Such "mass formulae" for local fields and orders in fact hold in far more generality (in particular, for degrees other than 3); see [24], [8], and [9].

8.5 The mean size of the 3-torsion subgroups of class groups of quadratic fields

In this section we prove Davenport and Heilbronn's theorem on the average size of the 3-torsion subgroups of class groups of quadratic fields. This is accomplished using class field theory, as in Davenport and Heilbronn's original arguments. This will prove Corollary 7.

Let $\mathcal{V} = \cap_p \mathcal{V}_p$ be the set of all $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings that are nowhere totally ramified (as in Section 3). Then by Lemma 13, we have $\mu(\mathcal{V}_p) = (1 - p^{-2})^2$. By the same argument as in the proof of the main term of Theorem 2,

$$\lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12n_i} \prod[(1 - p^{-2})^2] = \frac{3}{n_i \pi^2}.$$

Now given a nowhere totally ramified cubic field K_3, we have observed earlier that in the Galois closure K_6 is contained a quadratic field K_2 and K_6/K_2 is unramified. In addition, the discriminant of K_2 is equal to the discriminant of K_3. Furthermore, by class field theory the number of triplets of cubic fields K_3 corresponding to a given K_2 in this way equals $(h_3^*(K_2) - 1)/2$, where $h_3^*(K_2)$ denotes the number of 3-torsion elements in the class group of K_2. Therefore,

$$\sum_{0 < \mathrm{Disc}(K_2) < X} (h_3^*(K_2) - 1)/2 = N(\mathcal{V} \cap V^{(0)}; X),$$

$$\sum_{-X < \mathrm{Disc}(K_2) < 0} (h_3^*(K_2) - 1)/2 = N(\mathcal{V} \cap V^{(1)}; X). \tag{58}$$

22

Since it is known that

$$\lim_{X \to \infty} \frac{\sum_{0 < \mathrm{Disc}(K_2) < X} 1}{X} = \frac{3}{\pi^2},$$

$$\lim_{X \to \infty} \frac{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1}{X} = \frac{3}{\pi^2},$$

(59)

we conclude

$$\lim_{X \to \infty} \frac{\sum_{0 < \mathrm{Disc}(K_2) < X} h_3^*(K_2)}{\sum_{0 < \mathrm{Disc}(K_2) < X} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(0)}; X)}{\sum_{0 < \mathrm{Disc}(K_2) < X} 1} = 1 + \frac{2 \cdot 3/6\pi^2}{3/\pi^2} = \frac{4}{3},$$

$$\lim_{X \to \infty} \frac{\sum_{-X < \mathrm{Disc}(K_2) < 0} h_3^*(K_2)}{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(1)}; X)}{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1} = 1 + \frac{2 \cdot 3/2\pi^2}{3/\pi^2} = 2.$$

9 A refined sieve, and proofs of Theorems 2–5

As we have seen, an integer binary cubic form corresponds to a maximal ring if and only if its coefficients satisfy certain congruence conditions modulo p^2 for each prime p. To prove Theorem 2 using Theorem 21, we require a suitable sieve as follows. For a squarefree integer n, define $\mathcal{W}_n = \cap_{p|n} \mathcal{W}_p$. Then the number of isomorphism classes of maximal orders having discriminant in the dyadic range $X/2$ to X is equal to

$$N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X) = \sum_{n \in \mathbb{N}} \mu(n) N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X).$$

(60)

In order to prove Theorem 2, we need to estimate the individual terms on the right hand side of (60) accurately. The difficulty lies in the fact that the sets $\mathcal{W}_n$ are defined by congruence conditions modulo n^2. We are then not able to effectively apply Theorem 21, due to the fact that the $\mathcal{W}_n$ is the union of a large number of lattices modulo n^2. In Section 9.1, we show how to transform this count to one over fewer lattices defined by congruence conditions modulo n, thus enabling us to use Theorem 21 more effectively.

We then split (60) into three ranges for n and use a different method on each range. We use the splitting of the discriminant range into dyadic ranges so that we may choose the three ranges for n depending on the dyadic range of the discriminant. When n is small, we use Theorem 21 together with the correspondence in Section 9.1 to evaluate $N(\mathcal{W}_n; X/2, X)$ with two main terms and a smaller error term. Meanwhile, when n gets very large we apply the uniformity estimates from [1, Lemma 2.7] to bound the size of $|N(\mathcal{W}_n; X/2, X)|$. Lastly, when n is around $X^{1/6}$ it turns out that Theorem 21 and [1, Lemma 2.7] do not suffice, and so we require a different argument. We use again the correspondence of Section 9.1 to reduce the problem to one of determining the main term for the weighted number of binary cubic forms having bounded discriminant, where each binary cubic form is weighted by the number of its roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$. To accomplish this count, we argue that the number of roots is equidistributed inside boxes of small size compared to n.

Finally in Section 9.6 we prove Theorem 5 by expressing the number of isomorphism classes of cubic rings of bounded discriminant satisfying specified local conditions in terms of local masses of cubic rings.

9.1 A useful correspondence

Define a 2-*dimensional cubic space* to be a pair (L, F), where L is a lattice of rank 2 over $\mathbb{Z}$ and F is a cubic form on L. Picking a basis $\langle \alpha, \beta \rangle$ for L yields a binary cubic form f defined by $f(x, y) = F(x\alpha + y\beta)$. The form f is well-defined up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence. We define the *discriminant* of the pair (L, F) by $\mathrm{Disc}(L, F) = \mathrm{Disc}(f)$. We say that (L, F) is an *integral* 2-*dimensional cubic space* if f has integer coefficients. We say that two integral 2-dimensional cubic spaces (L_1, F_1) and (L_2, F_2) are *isomorphic* if there exists an isomorphism $\psi : L_1 \to L_2$ such that $F_1(v) = F_2(\psi(v))$ for all $v \in L_1$. It is then clear that isomorphism

23

classes of integral 2-dimensional cubic spaces are in canonical bijection with $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms.

Let (L, F) be an integral 2-dimensional cubic space such that any corresponding integer binary cubic form f belongs to $\mathcal{W}_p \setminus p \cdot V_{\mathbb{Z}}$. Define $\phi_L : L \setminus pL \to \mathbb{P}(L/pL)$ via reduction modulo p followed by projectivization. Then, by Lemma 9, there exists a unique $\alpha \in \mathbb{P}(L/pL)$ such that if $v \in L \setminus pL$ satisfies $\phi_L(v) = \alpha$, then $F(v) \equiv 0 \pmod{p^2}$. Motivated by this, we say that a triple (L, F, α), where (L, F) is an integral 2-dimensional cubic space and α is in $\mathbb{P}(L/pL)$, is a *Type 1 triple* if $F(v) \equiv 0 \pmod{p^2}$ for any $v \in L \setminus pL$ satisfying $\phi_L(v) = \alpha$. We define the *discriminant* of a Type 1 triple (L, F, α) to be equal to the discriminant of (L, F). We say that two Type 1 triples (L_1, F_1, α_1) and (L_2, F_2, α_2) are *isomorphic* if: a) (L_1, F_1) and (L_2, F_2) are isomorphic, and b) if $\phi_{L_1}(v_1) = \alpha_1$, then under this isomorphism $v_1 \in L_1$ is mapped to some element $v_2 \in L_2$ satisfying $\phi_{L_2}(v_2) = \alpha_2$.

Next, given a Type 1 triple (L, F, α), we can define a new lattice $L' \subset L \otimes_{\mathbb{Z}} \mathbb{Q}$ containing L that is spanned by L and v/p for any element v such that $\phi_L(v) = \alpha$. The cubic form $F' := pF$ on L extends naturally to a cubic form on L', yielding an integral 2-dimensional cubic space (L', F'). Moreover, we obtain a well-defined element $\alpha' \in \mathbb{P}^1(L'/pL')$ by setting $\alpha' = \phi_{L'}(v')$ for any element $v' \in L$ such that $\langle v, v' \rangle$ span $L \subset L'$. Notice then that $F'(v') \equiv 0 \pmod{p}$.

We say that (L', F', α'), where (L', F') is an integral 2-dimensional cubic space and $\alpha' \in \mathbb{P}(L'/pL')$, is a *Type 2 triple* if $F'(v') \equiv 0 \pmod{p}$ for any v' such that $\phi_{L'}(v') = \alpha'$. We similarly define the *discriminant* of a Type 2 triple (L', F', α') to be equal to the discriminant of (L', F'). We say that two Type 2 triples (L_1', F_1', α_1') and (L_2', F_2', α_2') are isomorphic if: a) (L_1', F_1') and (L_2', F_2') are isomorphic, and b) if $\phi_{L_1'}(v_1') = \alpha_1'$, then under this isomorphism $v_1' \in L_1'$ is mapped to an element $v_2' \in L_2'$ satisfying $\phi_{L_2'}(v_2') = \alpha_2'$.

We thus have a natural map taking Type 1 triples to Type 2 triples. Given a Type 2 triple (L', F', α'), we can recover the Type I triple (L, F, α) in the following way. First, pick a basis (v_1', v_2') for L' in such a way that $\phi_{L'}(v_2') = \alpha'$. Then L is the lattice spanned by pv_1' and v_2', $F = p^{-1}F'$, and $\alpha = \phi_{L'}(pv_1')$. Therefore, our map from Type 1 triples to Type 2 triples is a bijection. Finally note that if a Type 1 triple (L, F, α) maps to a Type 2 triple (L', F', α'), then $\mathrm{Disc}(L, F, \alpha) = p^2 \cdot \mathrm{Disc}(L', F', \alpha')$.

We now count isomorphism classes of Type 1 triples having discriminant between 0 and X, as well as isomorphism classes of Type 2 triples having discriminant between 0 and X/p^2, and then equate the answers.

Counting Type 1 triples: First, note that a $\mathrm{GL}_2(\mathbb{Z})$-orbit on $\mathcal{W}_p \setminus p \cdot V_{\mathbb{Z}}$ corresponds to exactly one Type 1 triple. Furthermore, the $\mathrm{GL}_2(\mathbb{Z})$-orbit of $f = pf' \in p \cdot V_{\mathbb{Z}}$ corresponds to $\omega_p(f')$ Type 1 triples, where $\omega_p(f')$ is the number of roots in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ of $f' \pmod{p}$.

For $\alpha \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, we define $V_{p,\alpha}$ to be the set of all integer binary cubic forms $f \in V_{\mathbb{Z}}$ such that $f \pmod{p}$ has a root at α. Similarly, for any $n \in \mathbb{N}$ and $\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$, we define $V_{n,\alpha}$ to be the set of all integer binary cubic forms $f \in V_{\mathbb{Z}}$ such that the reduction of f modulo n has a root at α. Note that although $V_{p,\alpha}$ is not $\mathrm{GL}_2(\mathbb{Z})$-invariant, the union $\bigcup_\alpha V_{p,\alpha}$ is $\mathrm{GL}_2(\mathbb{Z})$-invariant.

From the above discussion, we see that the number of isomorphism classes of Type 1 triples having discriminant bounded by X is equal to

$$N(\mathcal{W}_p; X) - N(V_{\mathbb{Z}}; X/p^4) + \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^4). \tag{61}$$

The third term in the right hand side of the above equation counts those Type 1 triples that correspond to integer binary cubic forms in $p \cdot V_{\mathbb{Z}}$.

Counting Type 2 triples: The $\mathrm{GL}_2(\mathbb{Z})$-orbit of an integer binary cubic form f corresponds to $\omega_p(f)$ Type 2 triples. Thus the number of isomorphism classes of Type 2 triples having discriminant bounded by X/p^2 is

$$\sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^2). \tag{62}$$

Equating (61) and (62) we arrive at the following formula, which will be essential for us:

$$N(\mathcal{W}_p; X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^2) - \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^4) + N(V_{\mathbb{Z}}; X/p^4). \tag{63}$$

The above analysis generalizes in a straightforward way to squarefree integers n to give

$$N(\mathcal{W}_n; X) = \sum_{\substack{k,\ell,m \in \mathbb{Z}_{\geq 0} \\ k\ell m = n \\ \alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{X}{k^2 \ell^4 m^4}\right) = \sum_{\substack{k,\ell \in \mathbb{Z}_{\geq 0} \\ k\ell | n \\ \alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{Xk^2}{n^4}\right). \tag{64}$$

9.2 Back to the sieve

Let us define the error functions $E_n^{(i)}(X)$ and $E_n^{(i)}(X/2, X)$ for squarefree n by

$$
\begin{aligned}
E_n^{(i)}(X) &= N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X) - \gamma_1(n) c_1^{(i)} X + \gamma_2(n) c_2^{(i)} X^{5/6}, \\
E_n^{(i)}(X/2, X) &= N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X) - \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \left(1 - \frac{1}{2^{5/6}}\right) \gamma_2(n) c_2^{(i)} X^{5/6}\right),
\end{aligned} \tag{65}
$$

where $\gamma_1(n)$ and $\gamma_2(n)$ are defined by the conditions $\gamma_1(p) + \mu_1(p) = \gamma_2(p) + \mu_2(p) = 1$ for $n = p$ prime, and $\gamma_1(n) = \prod_{p|n} \gamma_1(p)$ and $\gamma_2(n) = \prod_{p|n} \gamma_2(p)$ for general squarefree n. Returning to Equation (60), we write

$$
\begin{aligned}
N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X) &= \sum_{n \in \mathbb{N}} \mu(n) N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X) \\
&= \sum_{n \in \mathbb{N}} \mu(n) \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \left(1 - \frac{1}{2^{5/6}}\right) \gamma_2(n) c_2^{(i)} X^{5/6}\right) + \sum_{n \in \mathbb{N}} \mu(n) E_n^{(i)}(X/2, X) \\
&= \frac{c_1^{(i)} X}{2\zeta(2)\zeta(3)} + \left(1 - \frac{1}{2^{5/6}}\right) \frac{c_2^{(i)} X^{5/6}}{\zeta(2)\zeta(5/3)} + \sum_{n \in \mathbb{N}} \mu(n) E_n^{(i)}(X/2, X).
\end{aligned}
$$

Thus to prove Theorem 2, it is sufficient prove the estimate

$$\sum_{n \in \mathbb{N}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6 - 1/48 + \epsilon}). \tag{66}$$

Fix small numbers $\delta_1, \delta_2 > 0$ to be determined later. We break up (66) into the three different ranges

$$0 \leq n \leq X^{1/6 - \delta_1}, \ X^{1/6 - \delta_1} \leq n \leq X^{1/6 + \delta_2}, \text{ and } X^{1/6 + \delta_2} \leq n$$

and estimate $\sum_n |E_n^{(i)}(X/2, X)|$ for n in each range separately.

9.3 The small and large ranges

Suppose n is a fixed positive integer. Let k, ℓ be positive integers such that $k\ell \mid n$ and let $\alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})$. Then, by Theorem 21, there exist constants $c_1^{(i)}(\alpha)$ and $c_2^{(i)}(\alpha)$ such that

$$N\left(V_{k\ell,\alpha} \cap V_{\mathbb{Z}}^{(i)}; \frac{Xk^2}{2n^4}, \frac{Xk^2}{n^4}\right) = c_1^{(i)}(\alpha) \frac{Xk^2}{2n^4} + \left(1 - \frac{1}{2^{5/6}}\right) c_2^{(i)}(\alpha) \left(\frac{Xk^2}{n^4}\right)^{5/6} + O_\epsilon\left(\frac{m_1^{1/3} X^{3/4 + \epsilon} k^{3/2}}{n^3}\right), \tag{67}$$

25

where, in the notation of Theorem 21, $m_1 = m_1(k, \ell, \alpha)$ is an integer dividing $k\ell$ which depends only on the lattice $V_{k\ell, \alpha}$. Now the number of lattices $V_{k\ell, \alpha}$ satisfying $m_1(k, \ell, \alpha) = d$ is bounded by $O(n^{1+\epsilon}/d)$. Therefore, from (64), (65), and (67), we see that

$$|E_n^{(i)}(X/2, X)| = O_\epsilon \left(\sum_{d|n} \frac{n^{1+\epsilon} d^{1/3} X^{3/4+\epsilon}}{dn^{3/2}} \right) = O_\epsilon \left(\frac{X^{3/4+\epsilon}}{n^{1/2-\epsilon}} \right).$$

Summing over n, we conclude that

$$\sum_{n=0}^{X^{1/6-\delta_1}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6 - \delta_1/2 + \epsilon}). \tag{68}$$

From the definitions of γ_1 and γ_2, and from (55), we have the estimates

$$\gamma_1(n) = O_\epsilon(n^{-2+\epsilon}) \text{ and } \gamma_2(n) = O_\epsilon(n^{-5/3+\epsilon}).$$

From [1, Lemma 2.7], which is an easy generalization of Proposition 23, we also have the estimate

$$N(\mathcal{W}_n; X) = O_\epsilon(X/n^{2-\epsilon}).$$

We deduce that

$$|E_n^{(i)}(X/2, X)| = O_\epsilon(X/n^{2-\epsilon}) + O_\epsilon(X^{5/6}/n^{5/3-\epsilon}),$$

and summing up over n we obtain

$$\sum_{n \geq X^{1/6+\delta_2}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6 - \delta_2 + \epsilon}) + O_\epsilon(X^{13/18 - 2\delta_2/3 + \epsilon}). \tag{69}$$

In the next section, we estimate the sum of $|E_n^{(i)}(X/2, X)|$ over the range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$.

9.4 An equidistribution argument

We now concentrate on the middle range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$. Let us write

$$N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X) = \sum_{km|n} \mu(m) S_{km}^{(i)}(Xk^2/n^4), \tag{70}$$

where

$$S_n^{(i)}(X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})} N(V_{n,\alpha} \cap V_{\mathbb{Z}}^{(i)}, X).$$

In this section, we estimate $S_n^{(i)}(X)$, and then use (65) and (70) to obtain a corresponding estimate on $E_n^{(i)}(X/2, X)$. Given a form f, let $w_n(f)$ denote as before the number of roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ of $f \pmod{n}$. Then the number $S_n^{(i)}(X)$ counts the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms in $V_{\mathbb{Z}}^{(i)}$, weighted by $w_n(f)$, having discriminant bounded by X. Thus

$$S_n^{(i)}(X) = \sum_{\substack{f \in \mathrm{GL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}^{\mathrm{irr}} \\ |\mathrm{Disc}(f)| \leq X}} w_n(f). \tag{71}$$

We now consider $w_n(f)$ as a function on $V_{\mathbb{Z}/n\mathbb{Z}}$ and bound its Fourier transform pointwise. This will allow us to show that $w_n(f)$ is equidistributed in boxes whose side lengths are small compared to n. This in turn will alllow us to count the number of binary cubic forms f, weighted by $w_n(f)$, in small boxes. We then

26

can count this weighted number of binary cubic forms in fundumental domains using the ideas of Section 5, yielding the desired estimate for $S_n^{(i)}(X)$, and therefore for $|E_n^{(i)}(X/2, X)|$.

For ease of notation, we denote $V_{\mathbb{Z}}$ by L from hereon in. Define $\widehat{L/nL}$ to be the space of additive characters $\chi : L \to \mathbb{C}^{\times}$. Then we define the Fourier transform $\widehat{g} : \widehat{L/nL} \to \mathbb{C}$ of a function $g : L/nL \to \mathbb{C}$ via

$$\widehat{g}(\chi) := n^{-4} \sum_{\ell \in L/nL} g(\ell)\chi(\ell).$$

Fourier inversion then states that

$$g(\ell) = \sum_{\chi \in \widehat{L/nL}} \hat{g}(\chi)\bar{\chi}(\ell).$$

We focus now on computing $\widehat{w_n}(\chi)$. Assume first that $n = p$ is prime. We start with the trivial character which maps all of L/pL to 1, which we denote by $\mathbb{1}$. Then

$$\widehat{w_p}(\mathbb{1}) = p^{-4} \sum_{\ell \in L/pL} w_p(\ell) = 1 + p^{-1}.$$

Now for any $\chi \neq \mathbb{1}$, we compute

$$
\begin{aligned}
\widehat{w_p}(\chi) &= p^{-4} \sum_{\ell \in L/pL} \chi(\ell)w_p(\ell) \\
&= p^{-4} \sum_{\ell : \chi(\ell)=1} w_p(\ell) + p^{-4} \sum_{\ell : \chi(\ell)\neq 1} w_p(\ell)\chi(\ell).
\end{aligned}
\tag{72}
$$

Since $\chi(\ell) = 1$ for p^3 values of ℓ and $w_p(\ell) \leq 3$ for $\ell \neq 0$, we have the estimate

$$\sum_{\ell : \chi(\ell)=1} w_p(\ell) \leq 3(p^3 - 1) + (p + 1) = 3p^3 + p - 2. \tag{73}$$

Because $w_p(\lambda\ell) = w_p(\ell)$ for any $\lambda \in \mathbb{F}_p^{\times}$, we see that if $\chi(\ell) \neq 1$ then

$$\sum_{\lambda \in \mathbb{F}_p^{\times}} w_p(\lambda\ell)\chi(\lambda\ell) = -w_p(\ell),$$

implying

$$\sum_{\ell : \chi(\ell)\neq 1} w_p(\ell)\chi(\ell) = -(p-1)^{-1} \sum_{\ell : \chi(\ell)\neq 1} w_p(\ell). \tag{74}$$

Combining (73) with (74), we see that (72) implies that

$$\widehat{w_p}(\chi) \ll p^{-1} \tag{75}$$

uniformly for $\chi \neq 0$.

Now let n be a general squarefree integer. Then $\widehat{L/nL} \cong \oplus_{p|n} \widehat{L/pL}$ and $w_n(f) = \prod_{p|n} w_p(f)$. From this we conclude that $\widehat{w_n}(\chi) = \prod_{p|n} \widehat{w_p}(\chi_p)$, where χ_p is the p-part of χ. Using this and (75) implies that

$$\widehat{w_n}(\chi) \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbb{1}}} p^{-1} \tag{76}$$

and also

$$\widehat{w_n}(\mathbb{1}) = \prod_{p|n}(1 + p^{-1}) = \sigma(n)/n, \tag{77}$$

27

where $\sigma(n)$ denotes as usual the sum-of-divisors function.

We now run through the argument in Section 5, counting integer binary cubic forms f weighted by $w_n(f)$. Identically as in (17), we have the following identity.

$$S_n^{(i)}(X) = \frac{1}{M_i} \int_{g \in N'(t)A'\Lambda} S_n^{(i)}(m, t, \lambda, X) t^{-2} dm\, d^\times t\, d^\times \lambda,\tag{78}$$

where

$$S_n^{(i)}(m, t, \lambda, X) := \sum_{x \in B(m,t,\lambda,X)} w_n(x).$$

To estimate $S_n^{(i)}(m, t, \lambda, X)$, we tile the set $B(m, t, \lambda, X)$ with boxes and count weighted integer cubic forms inside each box.

We have the following two lemmas.

Lemma 27 *Suppose R is a region in $\mathbb{R}^4$ having volume C_1 and surface area C_2. Let N be a positive integer. Then there exists a set $R' \subset R$ having volume equal to $C_1 + O(N \cdot C_2)$ such that R' can be tiled with 4-dimensional boxes of side length N.*

Proof: We first tile $\mathbb{R}^4$ with boxes having side length equal to N. Then we place R inside $\mathbb{R}^4$ and take R' to be the union of those boxes which lie entirely inside R. The region $R \setminus R'$ is within distance N of the boundary of R. It is thus clear that the volume of R' is equal to $C_1 + O(N \cdot C_2)$. $\square$

We now use equation (75) to establish the following quantitative equidistribution statement for $w_n(f)$ inside boxes having small sidelengths relative to n.

Lemma 28 *Let $\mathcal{B} \subset V$ be a box with sides parallel to the coordinate axes on V such that each side has length at most n. Then*

$$\sum_{v \in \mathcal{B}} w_n(v) = \frac{\sigma(n)}{n} \mathrm{Vol}(\mathcal{B}) + O_\epsilon(n^{3+\epsilon}).$$

Proof: Since each side length of $\mathcal{B}$ has side length at most n, we can consider the set of lattice points in $\mathcal{B}$ as a subset $\mathcal{B}_n$ of L/nL. We then use Fourier inversion to write

$$\sum_{v \in \mathcal{B} \cap V_{\mathbb{Z}}} w_n(v) = \sum_{v \in \mathcal{B}_n} \sum_{\chi \in \widehat{L/nL}} \widehat{w_n}(\chi) \bar{\chi}(v)\tag{79}$$

$$= N^4 \widehat{w_n}(\mathbb{1}) + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v).\tag{80}$$

There is a $v_0 \in L/nL$ such that $\mathcal{B}_n = \{(a_1, a_2, a_3, a_4) + v_0 \mid 0 \leq a_1, a_2, a_3, a_4 \leq N - 1\}$. For each χ, there are characters χ_i, for $1 \leq i \leq 4$, such that $\chi(a_1, a_2, a_3, a_4) = \prod_{i=1}^4 \chi_i(a_i)$. Then $\sum_{v \in \mathcal{B}_n} w_n(v)$ is equal to

$$N^4 \widehat{w_n}(\mathbb{1}) + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v) = N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \chi(-v_0) \prod_{i=1}^4 \sum_{a_i=0}^{N-1} \chi_i(-a_i).\tag{81}$$

We estimate the sum over each $\chi \neq \mathbb{1}$ separately. By (76), we know $|\widehat{w_n}(\chi)| \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbb{1}}} p^{-1}$. Now, for a character ψ of $\mathbb{Z}/n\mathbb{Z}$, we define $A_N(\psi)$ by

$$A_N(\psi) := \sum_{a=0}^{N-1} \psi(a) = \begin{cases} N & \psi = \mathbb{1} \\ \dfrac{1 - \psi(N)}{1 - \psi(1)} & \psi \neq \mathbb{1} \end{cases}$$

28

and then define $A_N(\chi) := \prod_{i=1}^4 A_N(\chi_i)$. This implies that $\displaystyle\sum_{\psi \in \mathbb{Z}/n\mathbb{Z}} |A_N(\psi)| \ll \sum_{k=1}^n \frac{n}{k} \ll n \log n$.

We now estimate the right hand side of (81) as follows:

$$N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi)\chi(-v) \prod_{i=1}^4 \sum_{a_i=0}^{N-1} \chi_i(-a_i) = N^4 \frac{\sigma(n)}{n} + O\Big(\sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} |A_N(\chi)\widehat{w_n}(\chi)| \Big)$$

$$= N^4 \frac{\sigma(n)}{n} + O_\epsilon(n^{3+\epsilon}),$$

where the last bound follows from

$$\sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} |A_N(\chi)\widehat{w_n}(\chi)| \leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \sum_{\substack{\chi \\ \chi_p \neq \mathbb{1} \, \forall p|d \\ \chi_p = \mathbb{1} \, \forall p \nmid d}} |A_N(\chi)|$$

$$\leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \Big(\Big(\sum_{\psi \in \widehat{\mathbb{Z}/d\mathbb{Z}}} |A_N(\psi)| \Big)^4 - N^4 \Big)$$

$$\leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \Big((N + O(d \log d))^4 - N^4 \Big)$$

$$\leq \sum_{\substack{d|n \\ 1<d}} O_\epsilon(\max(d, N)^{3+\epsilon})$$

$$\leq O_\epsilon(n^{3+\epsilon}).$$

This completes the proof of the lemma. $\square$

We now estimate $S_n^{(i)}(m, t, \lambda, X)$, for $|m| < 1/2$, as follows. First tile $B(m, t, \lambda, X)' \subset B(m, t, \lambda, X)$ with boxes using Lemma 27. Note that the region $B(m, t, \lambda, X)$ is obtained by acting on the region $B(1, 1, 1, \frac{X}{\lambda^4})$ by $m \cdot t \cdot \lambda \in \mathrm{GL}_2(\mathbb{R})$. So the surface area of $B(m, t, \lambda, X)$ is $O(\lambda^3 t^3)$. We thus have

$$S_n^{(i)}(m, t, \lambda, X) = \frac{\sigma(n)}{n}\mathrm{Vol}(B(m, t, \lambda, X)) + O_\epsilon\left(\frac{n^{3+\epsilon}\lambda^4}{N^4}\right) + O(\lambda^3 t^3 N), \tag{82}$$

where the first error term comes from Lemma 28 and the second comes from Lemma 27. We optimize by picking $N = \lambda^{1/5} t^{-3/5} n^{3/5}$. Using (82), as in Section 5, we evaluate the right hand side of (78) to obtain

$$S_n^{(i)}(X) = \frac{\sigma(n)}{n} c_1^{(i)} X + O_\epsilon(n^{3+\epsilon} + X^{5/6} n^{1/2}). \tag{83}$$

Using (64), (65), $\gamma_2(n) = O_\epsilon(n^{-5/3+\epsilon})$, and (83) we finally arrive at the bound

$$|E_n^{(i)}(X)| \leq \gamma_2(n) X^{5/6} + O_\epsilon(n^\epsilon)\Big(\sum_{\substack{k,\ell \in \mathbb{Z} \\ k\ell | n}} (k\ell)^3 + \frac{X^{5/6} k^{5/3}}{n^{17/6}} \Big).$$

Therefore, we have

$$|E_n^{(i)}(X)| = O_\epsilon(n^\epsilon)\Big(\frac{X^{5/6}}{n^{7/6}} + n^3 \Big)$$

implying

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X)| \ll_\epsilon X^{29/36 + \frac{\delta_1}{6} + \epsilon} + X^{2/3 + 4\delta_2 + \epsilon}. \tag{84}$$

29

This also implies the estimate

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X/2,X)| \ll_\epsilon X^{29/36+\frac{\delta_1}{6}+\epsilon} + X^{2/3+4\delta_2+\epsilon}. \tag{85}$$

9.5 Putting it together

We combine (68), (69) and (85) to obtain

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2,X)| \ll_\epsilon X^{5/6-\delta_1/2+\epsilon} + X^{29/36+\delta_1/6+\epsilon} + X^{2/3+4\delta_2+\epsilon} + X^{5/6-\delta_2+\epsilon} + X^{13/18-2\delta_2/3}.$$

We optimize by picking $\delta_1 = \frac{1}{24}$ and $\delta_2 = \frac{1}{30}$ to get

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2,X)| \ll_\epsilon X^{5/6-1/48+\epsilon},$$

which proves Theorem 2.

Finally, note that the values of $\mu_1(\sigma,p)$ and $\mu_2(\sigma,p)$ that we list in Table 1 are the same as the values of C_{p,α_p} and K_{p,α_p}, respectively, in [23, Equation (5.1)]. We thus also obtain Roberts' refined conjecture (see [23, Section 5]); the proof is now identical to the proof of Theorem 2.

9.6 Another simultaneous generalization

In this subsection, we prove Theorem 5.

Proof of Theorem 5: Let p be a fixed finite prime. If $R \in \Sigma_p$ is a cubic ring over $\mathbb{Z}_p$, then we define $V(R) \subset V_\mathbb{Z}$ to be the set of all integer binary cubic forms f such that the corresponding cubic ring C satisfies $C \otimes \mathbb{Z}_p \cong R$. As in Section 7, we define $\mu_1(R,p)$ and $\mu_2(R,p)$ to be such that

$$N(V(R) \cap V^{(i)}; X) = \mu_1(R,p)c_1^{(i)}X + \mu_2(R,p)c_2^{(i)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).$$

Using the same techniques as in the proof of Theorem 2, we have

$$\begin{aligned}
N(\Sigma;X) &= \Big(\tfrac{1}{2}\sum_{R\in\Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|}\Big) \cdot \prod_p \Big(\sum_{R\in\Sigma_p} \mu_1(R,p)\Big) \cdot \zeta(2) \cdot X \\
&+ \Big(\sum_{R\in\Sigma_\infty} c_2(R)\Big) \cdot \prod_p \Big(\sum_{R\in\Sigma_p} \mu_2(R,p)\Big) \cdot X^{5/6} \\
&+ O_\epsilon(X^{5/6-1/48+\epsilon}).
\end{aligned} \tag{86}$$

We now prove the following lemma:

Lemma 29 *With notation as above, we have*

$$\mu_2(R,p) = (1-p^{-2})(1-p^{-1/3})\Big(\frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3}dx\Big).$$

Proof: Fix a form $f \in V_{\mathbb{Z}_p}$ corresponding to R. Let m be a positive integer such that p^m is larger than $\mathrm{Disc}_p(R)$, so that in particular $\mathrm{Disc}(f) \not\equiv 0 \pmod{p^m}$. Let $F = \{f_1, f_2, \ldots, f_r\}$ be the $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-orbit of the reduction of $f \pmod{p^m}$. By the slicing techniques of Section 6, as used in the proof of Theorem 21, we have

$$\mu_2(R,p) = p^{-3m} \cdot \left.\frac{\sum_{i=1}^r \sum_{a\equiv a(f_i)} a^{-s}}{\sum_{a\neq 0} a^{-s}}\right|_{s=1/3},$$

30

where $a(f_i)$ is the coefficient of x^3 in f_i and the congruences are taken modulo p^m. Since F is $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-invariant, every value of $a(f_i)$ with the same p-adic valuation occurs equally often in F. Therefore, we have

$$\mu_2(R,p) = (1 - p^{-1/3})p^{-3m} \sum_{i=1}^{r} \begin{cases} \dfrac{p^{1-m}|a(f_i)|_p^{-2/3}}{p-1} & \text{if } a(f_i) \neq 0 \\[2ex] \dfrac{p^{-m/3}}{1 - p^{-1/3}} & \text{if } a(f_i) = 0. \end{cases} \tag{87}$$

The group $\mathrm{GL}_2(\mathbb{Z}_p)$ acts on f in the natural way. Normalizing the Haar measure so as to give $\mathrm{GL}_2(\mathbb{Z}_p)$ measure 1, we rewrite (87) as

$$\mu_2(R,p) = \frac{(1-p^{-2})(1-p^{-1/3})}{|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|} \cdot \int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg.$$

Now, by computing the measure of $\mathrm{GL}_2(\mathbb{Z}_p) \cdot f$ in two different ways, we obtain

$$\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f) = \mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f) \cdot \mathrm{Disc}_p(f).$$

The first method is by splitting $\mathrm{GL}_2(\mathbb{Z}_p) \cdot f$ into $p^m \cdot V_{\mathbb{Z}_p}$ cosets. The number of such cosets is exactly $|\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})| \cdot |\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|^{-1}$. The second method is by integrating over the group, and using that the left invariant measure on $V_{\mathbb{Z}_p}$ is $|\mathrm{Disc}(v)|^{-1}dv$ and the map $g \to g \cdot f$ is a $|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)(f)}|$-to-1 cover.

We thus have

$$\mu_2(R,p) = \frac{(1-p^{-2})(1-p^{-1/3})}{\mathrm{Disc}_p(f) \cdot |\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f)|} \cdot \int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg.$$

Note that $a(g \cdot f) = f(v_0 \cdot g)$ where $v_0 = (1,0) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Therefore, we have

$$\int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg = \int_{(\mathbb{Z}_p^2)^{\mathrm{Prim}}} |f(v)|_p^{-2/3} dv,$$

where dv is normalized to have measure 1 on $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$.

From the correspondence in Section 2, we see that the set $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponds to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$ and that for $v \in (\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponding to $x \in R$, the value of $f(v)$ is equal to the index of $\mathbb{Z}[x]$ in R. Therefore the lemma follows. $\square$

Theorem 5 now follows from Theorem 25 and the above lemma. $\square$

Acknowledgments

References

[1] K. Belabas, M. Bhargava, and C. Pomerance, Error terms for the Davenport-Heilbronn theorems, *Duke Math. J.* **153** (2010), 173-210.

[2] K. Belabas, On the mean 3-rank of quadratic fields, *Compositio Math.* **118** (1999), no. 1, 1–9. Corrigendum: "On the mean 3-rank of quadratic fields," *Compositio Math.* **140** (2004), p. 1221.

[3] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), no. 219, 1213–1237.

[4] K. Belabas, E. Fouvry, Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, *Duke Math. J.* **98** (1999), no. 2, 217–268.

[5] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Annals of Math.* **159** (2004), no. 1, 217–250.

[6] M. Bhargava, The density of discriminants of quartic rings and fields, *Annals of Math.* **162** (2005), 1031–1063.

[7] M. Bhargava, The density of discriminants of quintic rings and fields, *Annals of Math.*, to appear.

[8] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Internat. Math. Res. Not.*, IMRN 2007, no. 17, Art. ID rnm052, 20 pp.

[9] M. Bhargava, Mass formulae for algebras over $\mathbb{F}_p$ and over $\mathbb{Q}_p$, in progress.

[10] M. Bhargava and A. Shnidman, On the number of cubic orders of bounded discriminant having automorphic group C_3, and related problems, in preparation.

[11] M. Bhargava and M. M. Wood, The density of discriminants of S_3-sextic number fields, *Proc. Amer. Math. Soc.* **136** (2008), no. 5, 1581–1587.

[12] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.* **386** (1988), 116–138.

[13] H. Davenport, On a principle of Lipshitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz", *J. London Math. Soc.* **39** (1964), 580.

[14] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[15] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[16] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[17] W. Duke and E. Kowalski, A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations (with an appendix by Dinakar Ramakrishnan), *Invent. Math.* **139** (2000), no. 1, 1–39.

[18] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications, *J. Reine Angew. Math.* **540** (2001), 115–166.

[19] G. W. Fung and H. C. Williams, On the computation of a table of complex cubic fields with discriminant $D > -10^6$, *Math. Comp.* **55** (1990), no. 191, 313–325.

[20] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), 105–169.

[21] P. Llorente and J. Quer, On totally real cubic fields with discriminant $D < 10^7$, *Math. Comp.* **50** (1988), no. 182, 581–594.

[22] A. W. Knapp, *Lie groups beyond an introduction*, Second ed., Progress in Mathematics, 140, Birkhäuser, Boston, 2002.

[23] D. P. Roberts, Density of cubic field discriminants, *Math. Comp.* **70** (2001), no. 236, 1699–1705 (electronic).

[24] J-P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, *C. R. Acad. Sci. Paris* Sér. A-B **286** (1978), no. 22, A1031–A1036.

[25] M. Sato and T. Shintani, On zeta functions associated with prehomogeneous vector spaces, *Annals of Math.* (2) **100** (1974), 131–170.

[26] T. Shintani, On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), 132–188.

[27] V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* **311** (1998), 791–794.

[28] S. Wong, Elliptic curves and class number divisibility, *Internat. Math. Res. Notices* **1999**, no. 12, 661–672.

[29] M. Wood, Moduli spaces for rings and ideals, Ph.D. Thesis, Princeton University, June 2009.

On the Davenport-Heilbronn theorem and second order terms

Manjul Bhargava, Arul Shankar, and Jacob Tsimerman

June 1, 2010

1 Introduction

The classical theorem of Davenport and Heilbronn [16] provides an asymptotic formula for the number of cubic fields having bounded discriminant. Specifically, the theorem states:

Theorem 1 (Davenport–Heilbronn) *Let $N_3(\xi, \eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$
\begin{aligned}
N_3(0, X) &= \frac{1}{12\zeta(3)}X &+& \quad o(X), \\
N_3(-X, 0) &= \frac{1}{4\zeta(3)}X &+& \quad o(X).
\end{aligned}
\tag{1}
$$

The Davenport–Heilbronn theorem, and the methods underlying its proof, have seen applications in numerous works (see, e.g., [3], [4], [6], [11], [18], [19], [28], [29]).

Subsequent to their 1971 paper, extensive computations were undertaken by a number of authors (see, e.g., Llorente–Quer [22] and Fung–Williams [20]) in an attempt to numerically verify the Davenport–Heilbronn theorem. However, computations up to discriminants even as large as 10^7 were found to agree quite poorly with the theorem. This in turn led to questions about the magnitude of the error term in this theorem, and the problem of determining a precise second order term.

In a related work, Belabas [3] developed a method to enumerate cubic fields very fast—indeed, in essentially linear time with the discriminant—allowing him to make tables of cubic fields up to absolute discriminant 10^{11}. These computations still seemed to agree rather poorly with the Davenport–Heilbronn theorem, and led Belabas to only guess the existence of an error term smaller than $O(X/(\log X)^a))$ for any a. However, Belabas [2] later obtained the first subexponential error term of the form $O(X \exp(-\sqrt{\log X \log \log X}))$.

In 2000, Roberts [24] conducted a remarkable study of these latter computations in conjunction with certain theoretical considerations, which led him to conjecture a precise *second main term* in the Davenport–Heilbronn theorem. This conjectural second main term took the form of a certain explicit constant times $X^{5/6}$. Further computations carried out in the last few years have revealed Roberts' conjecture to agree extremely well with the data. Meanwhile, on the theoretical side, a power-saving error term was finally obtained by Belabas, the first author, and Pomerance [1], who showed an error term of $O(X^{7/8+\epsilon})$.

The purpose of the current article is to prove the above conjecture of Roberts. More precisely, we prove the following theorem.

Theorem 2 *Let $N_3(\xi, \eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$
\begin{aligned}
N_3(0, X) &= \frac{1}{12\zeta(3)}X &+& \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} &+& O_\epsilon(X^{5/6-1/48+\epsilon}), \\
N_3(-X, 0) &= \frac{1}{4\zeta(3)}X &+& \frac{\sqrt{3}\cdot 4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} &+& O_\epsilon(X^{5/6-1/48+\epsilon}).
\end{aligned}
\tag{2}
$$

1

Davenport and Heilbronn also proved a refined version of Theorem 1, where they give the asymptotics for the number of cubic fields K having bounded discriminant satisfying any specified set of splitting conditions at finitely many primes. Roberts also conjectures a precise second main term for the number of such fields K having discriminant bounded by X (see [24, Section 5]). We also prove Roberts' refined conjecture in Section 9.

In the process, we present a simpler approach to proving the original Davenport–Heilbronn theorem, and also a simpler approach to establishing the theorem of Davenport [15] on the density of discriminants of binary cubic forms. The second main term of the latter theorem of Davenport (who obtained only a second term of $O(X^{15/16})$) was first discovered by Shintani [27] using Sato and Shintani's theory of zeta functions for prehomogeneous vector spaces [26]. In this article, we also give an elementary derivation of this second main term of Shintani. More precisely, we prove:

Theorem 3 (Davenport–Shintani) *Let $N(\xi, \eta)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integer-coefficient binary cubic forms f satisfying $\xi < \mathrm{Disc}(f) < \eta$. Then*

$$
\begin{aligned}
N(0, X) &= \frac{\pi^2}{72} X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
N(-X, 0) &= \frac{\pi^2}{24} X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
\tag{3}
$$

In order to prove Theorem 2, we need (in particular) to apply a new, stronger version of Theorem 3 where we count equivalence classes of binary cubic forms satisfying any finite or other suitable set of congruence conditions. Such a theorem was obtained by Davenport–Heilbronn but their method does not yield second main terms. Meanwhile, Shintani's zeta function method does not immediately apply to cubic forms satisfying given congruence conditions. We prove this congruence version of Theorem 3 in Section 6.

In fact, we use this more general version of Theorem 3 to prove a generalization of Theorem 2 that also allows us to count cubic orders satisfying certain specified sets of local conditions. To state this more general theorem, we first restate Theorem 3 as:

Theorem 4 *Let $M_3(\xi, \eta)$ denote the number of isomorphism classes of orders R in cubic fields that satisfy $\xi < \mathrm{Disc}(R) < \eta$. Then*

$$
\begin{aligned}
M_3(0, X) &= \frac{\pi^2}{72} X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
M_3(-X, 0) &= \frac{\pi^2}{24} X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
\tag{4}
$$

The proof of Theorem 4 is relatively straightforward, given Theorem 3 and the "Delone–Faddeev bijection" between isomorphism classes of cubic orders and $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms (which we describe in more detail in Section 2).

The generalization of Theorem 2 (which will also then include Theorem 4) that we will prove allows one to count cubic orders of bounded discriminant satisfying any desired finite (or, in many natural cases, infinite) sets of local conditions. To state the theorem, for each prime p let Σ_p be any set of isomorphism classes of orders in étale cubic algebras over $\mathbb{Q}_p$; also, let Σ_∞ denote any set of isomorphism classes of étale cubic algebras over $\mathbb{R}$ (i.e., $\Sigma_\infty \subseteq \{\mathbb{R}^3, \mathbb{R} \oplus \mathbb{C}\}$). We say that the collection $(\Sigma_p) \cup \Sigma_\infty$ is *acceptable* if, for all sufficiently large primes p, the set Σ_p contains all maximal cubic orders over $\mathbb{Z}_p$—or at least those maximal cubic orders that are not totally ramified. We say that the collection $(\Sigma_p) \cup \Sigma_\infty$ is *strongly acceptable* if, for all sufficiently large primes p, the set Σ_p either consists of the set all maximal cubic orders over $\mathbb{Z}_p$ or the set of all cubic orders over $\mathbb{Z}_p$.

We wish to asymptotically count the total number of cubic orders R of absolute discriminant less than X that agree with such local specifications, i.e., $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. This asymptotic count—with the first *two* main terms—is contained in the following theorem:

2

Theorem 5 *Let $(\Sigma_p) \cup \Sigma_\infty$ be a strongly acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. For a free $\mathbb{Z}_p$-module M, define $M^{\mathrm{Prim}} \subset M$ by $M^{\mathrm{Prim}} := M \backslash \{p \cdot M\}$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$
N_3(\Sigma; X) = \Big(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|} \Big) \cdot \prod_p \Big(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \Big) \cdot X
$$

$$
+ \quad \frac{1}{\zeta(2)} \Big(\sum_{R \in \Sigma_\infty} c_2(R) \Big) \cdot \prod_p \Big((1 - p^{-1/3}) \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3} dx \Big) \cdot X^{5/6}
$$

$$
+ \quad O_\epsilon(X^{5/6 - 1/48 + \epsilon}),
$$

$$(5)$$

where $\mathrm{Disc}_p(R)$ denotes the discriminant of R over $\mathbb{Z}_p$ as a power of p, $i(x)$ denotes the index of $\mathbb{Z}_p[x]$ in R, dx assigns measure 1 to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$, and

$$
c_2(R) = \begin{cases} c_2^{(0)} := \dfrac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}, \\[2ex] c_2^{(1)} := \dfrac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{C}. \end{cases}
$$

Note that the case where Σ_p consists of the maximal cubic orders over $\mathbb{Z}_p$ for all p yields Theorem 1, and also yields a corresponding interpretation of the asymptotic constants in Theorem 1 as a product of local Euler factors. Indeed, these Euler factors correspond to local weighted counts of the possible cubic algebras that can arise over $\mathbb{Q}_p$ and over $\mathbb{Q}_\infty = \mathbb{R}$.

Meanwhile, the case where Σ_p consists of all orders in étale cubic algebras over $\mathbb{Q}_p$ yields Theorem 4, and again also yields the analogous interpretation of the constants in Theorem 4. Theorem 5 thus simultaneously generalizes Theorems 2 and 4 in a natural way, and moreover, it yields a natural interpretation of the various constants $\frac{\pi^2}{72}$, $\frac{\pi^2}{24}$, $\frac{1}{12\zeta(3)}$, $\frac{1}{4\zeta(3)}$, etc. that appear in the asymptotics of these theorems.

If we are only interested in the first main term, we have the following stronger result:

Theorem 6 *Let $(\Sigma_p) \cup \Sigma_\infty$ be an acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Q}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$
N_3(\Sigma; X) = \Big(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|} \Big) \cdot \prod_p \Big(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \Big) \cdot X + o(X). \quad (6)
$$

The case where, for all p, the set Σ_p consists of all maximal cubic rings that are not totally ramified at p yields the following corollary which is also due to Davenport and Heilbronn.

Corollary 7 *Let D denote the discriminant of a quadratic field and let $\mathrm{Cl}_3(D)$ denote the 3-torsion subgroup of the ideal class group $\mathrm{Cl}(D)$ of D. Then*

$$
\lim_{X \to \infty} \frac{\sum_{0 < D < X} \#\mathrm{Cl}_3(D)}{\sum_{0 < D < X} 1} = \frac{4}{3}, \qquad \lim_{X \to \infty} \frac{\sum_{-X < D < 0} \#\mathrm{Cl}_3(D)}{\sum_{-X < D < 0} 1} = 2.
$$

Our proofs of Theorems 1–6 and particularly Theorem 5, though perhaps similar in spirit to the original arguments of Davenport and Heilbronn, involve a number of new ideas and refinements both on the algebraic and the analytic side. First, we begin in Sections 2 and 3 by giving a much shorter and more elementary derivation of the "Davenport–Heilbronn correspondence" between maximal cubic orders and appropriate sets of binary cubic forms.

Second, we obtain the main term of the asymptotics of Theorem 3 in Section 5 by counting points not in a single fundamental domain, but on average in a continuum of fundamental domains, using a technique of [7]. This leads, in particular, to a uniform treatment of the cases of positive and negative discriminants. It also leads directly to stronger error terms; most notably, we obtain immediately an error term of $O(X^{5/6})$ for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms of discriminant less than X, improving on Davenport's original $O(X^{15/16})$. The $O(X^{5/6})$ term is seen to come from the "cusps" or "tentacles" of the fundamental regions.

Third, to more efficiently count points in the cusps of these fundamental regions, we introduce a "slicing and smoothing" technique in Section 6, which then allows us to keep track of precise second order terms and thus also prove the second main term of Theorem 3. The technique works equally well when counting points satisfying any finite set of congruence conditions (see Theorem 21).

Fourth, our use of the Delone–Faddeev correspondence (c.f. Section 2) allows us to give an elementary treatment of the analogue of Theorem 2 for orders, rather than just fields, as in Theorem 4 and in the cases of Theorem 5 where only finitely many local conditions are involved. We prove the main terms of Theorems 1–6 in Section 8, using a simplified computation of p-adic densities that is carried out in Section 4.

Finally—in order to treat the second term in cases where infinitely many local conditions are involved—we introduce a sieving method that allows one to preserve the second main terms even when certain natural infinite sets of congruence conditions are applied. This is accomplished in Section 9, using a computation of "second order p-adic densities" that is carried out in Section 7.

Remark. Readers interested only in our new simpler proofs of the main terms of the Davenport–Heilbronn theorems may safely skip Sections 6, 7 and 9, which constitute about a half of this paper. On the other hand, those interested in the new results on second main terms may wish to concentrate primarily on these sections.

2   The Delone–Faddeev correspondence

A *cubic ring* is any commutative ring with unit that is free of rank 3 as a $\mathbb{Z}$-module. We begin with a theorem of Delone–Faddeev [17] (as refined by Gan–Gross–Savin [21]) parametrizing cubic rings by $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms. Throughout this paper, we always use the "twisted" action of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms, i.e., an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x, y)$ by

$$(\gamma \cdot f)(x, y) = \frac{1}{\det(\gamma)} \cdot f((x, y) \cdot \gamma).$$

Theorem 8 ([17],[21]) *There is a natural bijection between the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings.*

Proof: Given a cubic ring R, let $\langle 1, \omega, \theta \rangle$ be a $\mathbb{Z}$-basis for R. Translating ω, θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega \cdot \theta \in \mathbb{Z}$. A basis satisfying the latter condition is called *normal*. If $\langle 1, \omega, \theta \rangle$ is a normal basis, then there exist constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$\begin{array}{rcl} \omega\theta & = & n \\ \omega^2 & = & m + b\omega - a\theta \\ \theta^2 & = & \ell + d\omega - c\theta. \end{array} \tag{7}$$

To the cubic ring R, associate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (7). The values of ℓ, m, n are subject to the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega \cdot \omega\theta$, which when multiplied out using (7), yield a system of equations that possess a unique solution for n, m, ℓ, namely

$$\begin{array}{rcl} n & = & -ad \\ m & = & -ac \\ \ell & = & -bd. \end{array} \tag{8}$$

4

If follows that any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (7) and (8), leads to a unique cubic ring $R = R(f)$.

Lastly, one observes by an explicit calculation that changing the $\mathbb{Z}$-basis $\langle \omega, \theta \rangle$ of $R/\mathbb{Z}$ by an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the corresponding binary cubic form $f(x, y)$ by that same element of $\mathrm{GL}_2(\mathbb{Z})$. Hence an isomorphism class of cubic rings determines a binary cubic form uniquely up to the action of $\mathrm{GL}_2(\mathbb{Z})$. This is the desired conclusion. $\square$

One finds by an explicit calculation using (7) and (8) that *the discriminant of the cubic ring $R(f)$ is precisely the discriminant of the binary cubic form f*; explicitly, it is given by

$$\mathrm{Disc}(R(f)) = \mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \tag{9}$$

Next, we observe that *the cubic ring $R(f)$ is an integral domain if and only if f is irreducible as a polynomial over $\mathbb{Q}$*. Indeed, if $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is reducible, then it has a linear factor, which (by a change of variable in $\mathrm{GL}_2(\mathbb{Z})$) we may assume is y; i.e., $a = 0$. In this case, (7) and (8) show that $\omega\theta = 0$, so $R(f)$ has zero divisors.

Conversely, if a cubic ring R has zero divisors, then there exists some element $\omega \in R$ such that $\langle 1, \omega \rangle$ spans a quadratic subring of R. Such an ω can be constructed as follows. Let α and β be two nonzero elements of R with $\alpha\beta = 0$, and let $\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$ be the characteristic polynomial of α. Multiplying both sides by β, we see that $c_3 = 0$, so that $\alpha(\alpha^2 + c_1\alpha + c_2) = 0$. If $\alpha^2 + c_1\alpha + c_2 = 0$, then we may let $\omega = \alpha$. Otherwise, note that $(\alpha^2 + c_1\alpha + c_2)^2 = c_2(\alpha^2 + c_1\alpha + c_2)$, so in that case we may set $\omega = \alpha^2 + c_1\alpha + c_2$, and $\omega^2 = c_2\omega$. Either way, we see that $\langle 1, \omega \rangle$ spans a quadratic subring of R.

Scaling ω by an integer if necessary, we may assume that ω is a primitive vector in the lattice $R \cong \mathbb{Z}^3$, and then extend $\langle 1, \omega \rangle$ to a basis $\langle 1, \omega, \theta \rangle$ of R. Normalizing this basis if needed, we then see in (7) that we must have $a = 0$, implying that the associated binary cubic form is reducible. We conclude that, under the Delone–Faddeev correspondence, integral domains correspond to irreducible binary cubic forms.

Other properties of the cubic ring $R(f)$ can also be read off easily from the binary cubic form f. For example, *the group of ring automorphisms of $R(f)$ is simply the stabilizer of f in $\mathrm{GL}_2(\mathbb{Z})$*; this follows directly from the proof of Theorem 8.

Finally, we note that the correspondence of Theorem 8, and the analogues of the above consequences, also hold for cubic algebras and binary cubic forms over other base rings such as $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, and $\mathbb{Z}_p$, with the identical proofs. This observation will also be very useful to us in later sections.

3   The Davenport–Heilbronn correspondence

A cubic ring is said to be *maximal* if it is not a subring of any other cubic ring. The first part of the Davenport–Heilbronn theorem [16] describes a bijection (known as the "Davenport–Heilbronn correspondence") between maximal cubic rings and certain special classes of binary cubic forms. In this section, we give a simple derivation of this bijection.

By the work of the previous section, in order to obtain the Davenport–Heilbronn correspondence we must simply determine which binary cubic forms f yield maximal rings $R(f)$ in the bijection given by (7) and (8). Now a cubic ring R is maximal if and only if the cubic $\mathbb{Z}_p$-algebra $R_p = R \otimes \mathbb{Z}_p$ is maximal for every p (this is because R is a maximal ring if and only if it is isomorphic to a product of rings of integers in number fields). The condition on R that $R \otimes \mathbb{Z}_p$ be a maximal cubic algebra over $\mathbb{Z}_p$ is called "maximality at p". The following lemma illustrates the ways in which a ring R can fail to be maximal at p:

Lemma 9 *Suppose R is not maximal at p. Then there is a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ of R such that at least one of the following is true:*

- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ *forms a ring*

- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ *forms a ring.*

Proof: Let $R' \supset R$ be any ring strictly containing R such that the index of R in R' is a multiple of p, and let $R_1 = R' \cap (R \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}])$. Then the ring R_1 also strictly contains R, and the index of R in R_1 is a power of p. By the theory of elementary divisors, there exist nonnegative integers $i \geq j$ and a basis $\langle 1, \omega, \theta \rangle$ of R such that

$$R_1 = \mathbb{Z} + \mathbb{Z}(\omega/p^i) + \mathbb{Z}(\theta/p^j). \tag{10}$$

If $i = 1$, we are done. Hence we assume $i > 1$.

We normalize the basis $\langle 1, \omega, \theta \rangle$ if necessary; this does not affect the truth of equation (10). Now suppose the multiplicative structure of R is given by (7) and (8). That the right side of (10) is a ring translates into the following congruence conditions on a, b, c, d:[1]

$$a \equiv 0 \pmod{p^{2i-j}}, \quad b \equiv 0 \pmod{p^i}, \quad c \equiv 0 \pmod{p^j}, \quad d \equiv 0 \pmod{p^{2j-i}}. \tag{11}$$

If $j = 0$, then replacing (i, j) by $(i - 1, j)$ maintains the truth of the above congruences, and R_1 as defined by (10) remains a ring. If $j > 0$, then we may replace (i, j) instead by $(i - 1, j - 1)$. Thus in a finite sequence of such moves, we arrive at $i = 1$, as desired. $\square$

The lemma implies that a cubic ring $R(f)$ can fail to be maximal at p in two ways: either (i) f is a multiple of p, or (ii) there is some $\mathrm{GL}_2(\mathbb{Z})$-transformation of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ such that a is a multiple of p^2 and b is a multiple of p.

Let $\mathcal{U}_p$ be the set of all binary cubic forms f not satisfying either of the latter two conditions. Then we have proven

Theorem 10 (Davenport–Heilbronn [16]) *The cubic ring $R(f)$ is maximal if and only if $f \in \mathcal{U}_p$ for all p.*

Note that our definition of $\mathcal{U}_p$ is somewhat simpler than that used by Davenport–Heilbronn (but is easily seen to be equivalent).

4 Local behavior and p-adic densities

In this section, we consider elements f in the spaces of binary cubic forms f over the integers $\mathbb{Z}$, the p-adic ring $\mathbb{Z}_p$, and the residue field $\mathbb{Z}/p\mathbb{Z}$. We denote these spaces by $V_{\mathbb{Z}}$, $V_{\mathbb{Z}_p}$, and $V_{\mathbb{F}_p}$ respectively.

Aside from the degenerate case $f \equiv 0 \pmod{p}$, any form $f \in V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) determines exactly three points in $\mathbb{P}^1_{\mathbb{F}_p}$, obtained by taking the roots of f reduced modulo p. For such a form f, define the symbol (f, p) by setting

$$(f, p) = (f_1^{e_1} f_2^{e_2} \cdots),$$

where the f_i's indicate the degrees of the fields of definition over $\mathbb{F}_p$ of the roots of f, and the e_i's indicate the respective multiplicities of these roots. There are thus five possible values of the symbol (f, p), namely, (111), (12), (3), (1^21), and (1^3). Furthermore, it is clear that if two binary cubic forms f_1, f_2 over $\mathbb{Z}$ (resp. $\mathbb{Z}_p$, $\mathbb{F}_p$) are equivalent under a transformation in $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$), then $(f_1, p) = (f_2, p)$. By $T_p(111), T_p(12)$, etc., let us denote the set of f such that $(f, p) = (111)$, $(f, p) = (12)$, etc.

By the definition of $R(f)$, the ring structure of the quotient ring $R(f)/(p)$ depends only on the $\mathrm{GL}_2(\mathbb{F}_p)$-orbit of f modulo p; hence the symbol (f, p) indicates something about the structure of the ring $R(f)$ when reduced modulo p. In fact, writing down the multiplication laws at one point of each of the five aforementioned $\mathrm{GL}_2(\mathbb{F}_p)$-orbits demonstrates that

$$(f, p) = (f_1^{e_1} f_2^{e_2} \cdots) \iff R(f)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots.$$

In particular, it follows that for $f \in \mathcal{U}_p$, the symbol (f, p) conveys precisely the splitting behavior of $R(f)$ at p. For example, if $(f, p) = (1^3)$ for $f \in \mathcal{U}_p$, then this means the maximal cubic ring $R(f)$ is totally ramified at p.

Now, for any set S in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) that is definable by congruence conditions, let us denote by $\mu(S) = \mu_p(S)$ the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ on V so that $\mu(V_{\mathbb{Z}_p}) = 1$. The following lemma determines the p-adic densities of the sets $T_p(\cdot)$:

---

[1]We follow here the convention that, for $e \leq 0$, we have $a \equiv 0 \pmod{p^e}$ for any integer a.

Lemma 11 *We have*

$$
\begin{aligned}
\mu(T_p(111)) &= \tfrac{1}{6}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(12)) &= \tfrac{1}{2}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(3)) &= \tfrac{1}{3}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(1^21)) &= \quad (p-1)\,p\,(p+1)\,/\,p^4 \\
\mu(T_p(1^3)) &= \quad (p-1)\,(p+1)\,/\,p^4
\end{aligned}
$$

Proof: Since the criteria for membership of f in a $T_p(\cdot)$ depend only on the residue class of f modulo p, it suffices to consider the situation over $\mathbb{F}_p$. We examine first $\mu(T_p(111))$. The number of unordered triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is $\frac{1}{6}(p+1)p(p-1)$. Furthermore, given such a triple of points, there is a unique binary cubic form, up to scaling, having this triple of points as its roots. Since the total number of binary cubic forms over $\mathbb{F}_p$ is p^4, it follows that $\mu(T_p(111)) = \frac{1}{6}\big[(p+1)p(p-1)\big](p-1)/\,p^4$, as given by the lemma.

Similarly, the number of unordered triples of points, one member of which is in $\mathbb{P}^1_{\mathbb{F}_p}$ while the other two are $\mathbb{F}_p$-conjugate in $\mathbb{P}^1_{\mathbb{F}_{p^2}}$, is given by $\frac{1}{2}(p+1)(p^2-p)$. We thus have $\mu(T_p(12)) = \frac{1}{2}\big[(p+1)(p^2-p)\big](p-1)/\,p^4$. Also, the number of unordered $\mathbb{F}_p$-conjugate triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_{p^3}}$ is $(p^3-p)/3$, and hence $\mu(T_p(3)) = \big[(p^3-p)\big](p-1)/\,p^4$.

Meanwhile, the number of pairs (x,y) of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is given by $(p+1)p$, so that the number of binary cubic forms over $\mathbb{F}_p$ having a double root at some point x and a single root at another point y is $[(p+1)p](p-1)$. Thus $\mu(T_p(1^21)) = \big[(p+1)p\big](p-1)/\,p^4$. Finally, the number of binary cubic forms over $\mathbb{F}_p$ having a triple root in $\mathbb{P}^1_{\mathbb{F}_p}$ is $(p+1)(p-1)$, yielding $\mu(T_p(1^3)) = (p+1)(p-1)/p^4$ as desired. $\square$

We next wish to determine the p-adic densities of the sets $\mathcal{U}_p$. Let $\mathcal{U}_p(\cdot)$ denote the subset of elements $f \in T_p(\cdot)$ such that $R(f)$ is maximal at p. If f is an element of $T_p(111)$, $T_p(12)$, or $T_p(3)$, then $R(f)$ is clearly maximal at p, as its discriminant is coprime to p. Thus $U_p(111) = T_p(111)$, $U_p(12) = T_p(12)$, and $U_p(3) = T_p(3)$. If a binary cubic form f is in $T_p(1^21)$ or $T_p(1^3)$, then it can clearly be brought into the form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $a \equiv b \equiv 0 \pmod{p}$, namely, by sending the unique multiple root of f in $\mathbb{P}^1_{\mathbb{F}_p}$ to the point $(1,0)$ via a transformation in $\mathrm{GL}_2(\mathbb{Z})$. Of all $f \in T_p(1^21)$ or $T_p(1^3)$ that have been rendered in such a form, a proportion of $1/p$ actually satisfy the congruence $a \equiv 0 \pmod{p^2}$ of condition (ii). Thus a proportion of $(p-1)/p$ of forms in $T_p(1^21)$ and in $T_p(1^3)$ correspond to cubic rings maximal at p. We have thus proven:

Lemma 12 *We have*

$$
\begin{aligned}
\mu(\mathcal{U}_p(111)) &= \tfrac{1}{6}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(12)) &= \tfrac{1}{2}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(3)) &= \tfrac{1}{3}\,(p-1)^2\,p\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(1^21)) &= \quad (p-1)^2\,(p+1)\,/\,p^4 \\
\mu(\mathcal{U}_p(1^3)) &= \quad (p-1)^2\,(p+1)\,/\,p^5\,.
\end{aligned}
$$

Following [16] let $\mathcal{V}_p$ denote the set of elements $f \in \mathcal{U}_p$ such that $(f,p) \neq (1^3)$. Then it is clear from the above arguments that the elements of $\mathcal{V}_p$ correspond to maximal orders in étale cubic algebras over $\mathbb{Q}$ in which p does not totally ramify. The set $\mathcal{V}_p$ plays an important role in understanding the 3-torsion in the class groups of cubic fields (see Section 8).

Using the fact that $\mathcal{U}_p$ is simply the union of the $\mathcal{U}_p(\sigma)$'s, and $\mathcal{V}_p$ is the union of the $\mathcal{U}_p(\sigma)$'s where $\sigma \neq (1^3)$, we obtain from Lemma 12:

Lemma 13 *We have*

$$
\begin{aligned}
\mu(\mathcal{U}_p) &= (p^3-1)(p^2-1)\,/\,p^5 \\
\mu(\mathcal{V}_p) &= (p^2-1)^2\,/\,p^4\,.
\end{aligned}
$$

5 The number of binary cubic forms of bounded discriminant

Let $V = V_{\mathbb{R}}$ denote the vector space of binary cubic forms over $\mathbb{R}$. Then the action of $\mathrm{GL}_2(\mathbb{R})$ on V has two nondegenerate orbits, namely the orbit $V^{(0)}$ consisting of elements having positive discriminant, and $V^{(1)}$ consisting of those having negative discriminant. In this section we wish to understand the number $N(V^{(i)}; X)$ of <u>irreducible</u> $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i)}$ having absolute discriminant less than X ($i = 0, 1$). In particular, we prove the following strengthening of Davenport's theorem on the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms having bounded discriminant:

Theorem 14 $N(V_{\mathbb{Z}}^{(0)}; X) = \dfrac{\pi^2}{72} \cdot X + O(X^{5/6})$; $N(V_{\mathbb{Z}}^{(1)}; X) = \dfrac{\pi^2}{24} \cdot X + O(X^{5/6})$.

5.1 Reduction theory

Let $\mathcal{F}$ denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$. Then $\mathcal{F}$ may be expressed in the form $\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', k \in K, \lambda \in \Lambda\}$, where

$$N'(a) = \{\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} : n \in \nu(a)\}, \quad A' = \{\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2}\}, \quad \Lambda = \{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0\} \quad (12)$$

and K is as usual the (compact) real special orthogonal group $\mathrm{SO}_2(\mathbb{R})$; here $\nu(a)$ is the union of either one or two subintervals of $[-\frac{1}{2}, \frac{1}{2}]$ depending only on the value of $a \in A'$.

For $i = 1, 2$, let n_i denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any element $v \in V_{\mathbb{R}}^{(i)}$ (by the correspondence of Theorem 8 over $\mathbb{R}$, we have $n_1 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^3) = 6$ and $n_2 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = 2$). Then for any $v \in V^{(i)}$, $\mathcal{F}v$ will be the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$. Since this union is not necessarily disjoint, $\mathcal{F}v$ is best viewed as a multiset, where the multiplicity of a point x in $\mathcal{F}v$ is given by the cardinality of the set $\{g \in \mathcal{F} \mid gv = x\}$. Evidently, this multiplicity is a number between 1 and n_i.

Even though the multiset $\mathcal{F}v$ is the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$, not all elements in $\mathrm{GL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}$ will be represented in $\mathcal{F}v$ exactly n_i times. In general, the number of times the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of an element $x \in V_{\mathbb{Z}}$ will occur in the multiset $\mathcal{F}v$ is given by $n_i/m(x)$, where $m(x)$ denotes the size of the stabilizer of x in $\mathrm{GL}_2(\mathbb{Z})$. Now the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an irreducible element $x \in V_{\mathbb{Z}}$ is either trivial or C_3. We conclude that, for any $v \in V_{\mathbb{R}}^{(i)}$, the product $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$ is exactly equal to the number of irreducible integer points in $\mathcal{F}v$ having absolute discriminant less than X, with the slight caveat that the (relatively rare—see Lemma 16) C_3-points are to be counted with weight $1/3$.

Now the number of such integer points can be difficult to count in a single such fundamental domain. The main technical obstacle is that the fundamental region $\mathcal{F}v$ is not compact, but rather has a cusp going off to infinity which in fact contains infinitely many points, including many irreducible points. We simplify the counting of such points by "thickening" the cusp; more precisely, we compute the number of points in the fundamental region $\mathcal{F}v$ by averaging over lots of such fundamental domains, i.e., by averaging over points v lying in a certain special compact subset B of some fixed ball in V.

5.2 Estimates on reducibility

We first consider the reducible elements in the multiset $\mathcal{R}_X(v) := \{w \in \mathcal{F}v : |\mathrm{Disc}(w)| < X\}$, where v is any vector in a fixed compact subset B of V. Note that if a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3$ satisfies $a = 0$, then it is reducible over $\mathbb{Q}$, since y is a factor. The following lemma shows that for binary cubic forms in $\mathcal{R}_X(v)$, reducibility with $a \neq 0$ does not occur very often.

Lemma 15 *Let $v \in B$ be any point of nonzero discriminant, where B is any fixed compact subset of V. Then the number of integral binary cubic forms $ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{R}_X(v)$ that are reducible with $a \neq 0$ is $O(X^{3/4+\epsilon})$, where the implied constant depends only on B.*

Proof: For an element $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{R}_X(v)$, we see via the description of $\mathcal{R}_X(v)$ as $N'A'K\Lambda v$, where $v \in B$ and $0 < \lambda < X^{1/4}$, that $a = O(X^{1/4})$, $ab = O(X^{1/2})$, $ac = O(X^{1/2})$, $ad = O(X^{1/2})$, $abc = O(X^{3/4})$, and $abd = O(X^{3/4})$. In particular, the latter estimates clearly imply that the total number of forms $f \in \mathcal{R}_X(v)$ with $a \neq 0$ and $d = 0$ is $O(X^{3/4+\epsilon})$.

Let us now assume $a \neq 0$ and $d \neq 0$. Then the above estimates show that the total number of possibilities for the triple (a, b, d) is $O(X^{3/4+\epsilon})$. Suppose the values a, b, d ($d \neq 0$) are now fixed, and consider the possible number of values of c such that the resulting form $f(x,y)$ is reducible. For $f(x,y)$ to be reducible, it must have some linear factor $rx + sy$, where $r, s \in \mathbb{Z}$ are relatively prime. Then r must be a factor of a, while s must be a factor of d; they are thus both determined up to $O(X^\epsilon)$ possibilities. Once r and s are determined, computing $f(-s, r)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a, b, d, r, s. Thus the total number of reducible forms $f \in \mathcal{R}_X(v)$ with $a \neq 0$ is $O(X^{3/4+\epsilon})$, as desired. $\square$

Lemma 16 *Let $v \in V$ be any point of positive discriminant. Then the number of C_3-points in $\mathcal{R}_X(v)$ is $O(X^{3/4+\epsilon})$, where the implied constant is independent of V.*

Proof: The number of C_3-points in $\mathcal{R}_X(v)$ is equal to the number of isomorphism classes of cubic rings having automorphism group C_3 and discriminant less than X. This number is thus independent of v, and so it suffices to prove the lemma for any single v.

We choose v to be the binary cubic form $x^3 - 3xy^2$. The reason for this choice is as follows. Every binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ has a naturally associated binary quadratic form, namely, the "Hessian covariant" $H_f(x,y) = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$. It is easy to see that if a binary cubic form f is acted upon by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then H_f is also acted upon by the same transformation. Now $H_v(x,y) = 9(x^2 + y^2)$, and so $\mathcal{F}H_v$ consists of the usual reduced (positive-definite) binary quadratic forms $Ax^2 + Bxy + Cy^2$, where $|B| \leq A \leq C$. Thus $\mathcal{F}v$ consists of binary cubic forms satisfying $|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd$.

Now if a binary cubic form f in $\mathcal{F}v$ has a nontrivial stabilizing element γ of order 3 in $\mathrm{SL}_2(\mathbb{Z})$, then γ will also stabilize its Hessian H_f. But the only reduced binary quadratic form, up to multiplication by scalars, having a nontrivial stabilizing element of order 3 is $x^2 + xy + y^2$. Therefore, any such C_3-type binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ in $\mathcal{F}v$ must satisfy

$$b^2 - 3ac = bc - 9ad = c^2 - 3bd.$$

From this we see that, if a, b, d are fixed, then there is at most one solution for c. As in the proof of Lemma 15, the total number of possibilities for the triple (a, b, d) in $\mathcal{F}v$ is $O(X^{3/4+\epsilon})$, and the lemma follows. $\square$

In fact, by refining the proof of Lemma 16, it can be shown that the number of C_3-points in $\mathcal{R}_X(v)$ of discriminant less than X is asymptotic to $cX^{1/2}$, where $c = \sqrt{3}/18$; see [10].

Thus, as far as Theorem 14 is concerned, the C_3-points in $V_\mathbb{Z}$ are negligible in number and are absorbed in the error term.

5.3 Averaging

Let $B = B(C) = \{w = (a, b, c, d) \in V : 3a^2 + b^2 + c^2 + 3d^2 \leq C, |\mathrm{Disc}(w)| \geq 1\}$; $C = 10$ will suffice in what follows. Let $V_\mathbb{Z}^{\mathrm{irr}}$ denote the subset of irreducible points of $V_\mathbb{Z}$. Then we have

$$N(V^{(i)}; X) = \frac{\int_{v \in B \cap V^{(i)}} \#\{x \in \mathcal{F}v \cap V_\mathbb{Z}^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\} \, |\mathrm{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv}. \tag{13}$$

The denominator of the latter expression is, by construction, a finite absolute constant greater than zero. We have chosen the measure $|\mathrm{Disc}(v)|^{-1} \, dv$ because it is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure.

More generally, for any $\mathrm{GL}_2(\mathbb{Z})$-invariant subset $S \subset V_\mathbb{Z}^{(i)}$, let $N(S; X)$ denote the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on S having discriminant less than X. Let S^{irr} denote the subset of irreducible points

of S. Then $N(S; X)$ can be expressed as

$$N(S; X) = \frac{\int_{v \in B \cap V^{(i)}} \#\{x \in \mathcal{F}v \cap S^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\} \, |\mathrm{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv}. \tag{14}$$

We shall use this definition of $N(S; X)$ for any $S \subset V_{\mathbb{Z}}$, even if S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant. Note that for disjoint $S_1, S_2 \subset V_{\mathbb{Z}}$, we have $N(S_1 \cup S_2) = N(S_1) + N(S_2)$.

Now since $|\mathrm{Disc}(v)|^{-1} dv$ is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure, we have for any $f \in C_0(V^{(i)})$ and $x \in V^{(i)}$ that $\int_{V^{(i)}} f(v)|\mathrm{Disc}(v)|^{-1} dv = \int_G c_i f(gx) \, dg$ for some constant c_i dependent only on whether $i = 0$ or 1; here dg denotes a left-invariant Haar measure on $G = \mathrm{GL}_2(\mathbb{R})$. We may thus express the above formula for $N(S; X)$ as an integral over $\mathcal{F} \subset \mathrm{GL}_2(\mathbb{R})$:

$$N(S; X) = \frac{1}{M_i} \int_{g \in \mathcal{F}} \#\{x \in S^{\mathrm{irr}} \cap gB : |\mathrm{Disc}(x)| < X\} \, dg \tag{15}$$

$$= \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda K} \#\{x \in S^{\mathrm{irr}} \cap n \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \lambda k B : |\mathrm{Disc}(x)| < X\} t^{-2} dn \, d^{\times} t \, d^{\times} \lambda \, dk. \tag{16}$$

where

$$M_i = \frac{n_i}{2\pi} \cdot \int_{v \in B \cap V^{(i)}} |\mathrm{Disc}(v)|^{-1} dv.$$

We note that the constant 2π comes from the change of measure $|\mathrm{Disc}(v)|^{-1} dv$ to dg, as will be seen in Proposition 19. Let us write $B(n, t, \lambda, X) = n \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \lambda B \cap \{v \in V^{(i)} : |\mathrm{Disc}(v)| < X\}$. As $KB = B$ and $\int_K dk = 1$, we have

$$N(S; X) = \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X)\} t^{-2} dn \, d^{\times} t \, d^{\times} \lambda. \tag{17}$$

To estimate the number of lattice points in $B(n, t, \lambda, X)$, we have the following two elementary propositions from the geometry-of-numbers. The first is essentially due to Davenport [14]. To state the proposition, we require the following simple definitions. A multiset $\mathcal{R} \subset \mathbb{R}^n$ is said to be *measurable* if $\mathcal{R}_k$ is measurable for all k, where $\mathcal{R}_k$ denotes the set of those points in $\mathcal{R}$ having a fixed multiplicity k. Given a measurable multiset $\mathcal{R} \subset \mathbb{R}^n$, we define its volume in the natural way, that is, $\mathrm{Vol}(\mathcal{R}) = \sum_k k \cdot \mathrm{Vol}(\mathcal{R}_k)$, where $\mathrm{Vol}(\mathcal{R}_k)$ denotes the usual Euclidean volume of $\mathcal{R}_k$.

Proposition 17 *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\bar{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on n, m, k, and ℓ.

Although Davenport states the above lemma only for compact semi-algebraic sets $\mathcal{R} \subset \mathbb{R}^n$, his proof adapts without essential change to the more general case of a bounded semi-algebraic multiset $\mathcal{R} \subset \mathbb{R}^n$, with the same estimate applying also to any image $\mathcal{R}'$ of $\mathcal{R}$ under a unipotent triangular transformation.

We now have the following lemma on the number of irreducible lattice points in $B(n, t, \lambda, X)$:

Lemma 18 *The number of lattice points (a, b, c, d) in $B(n, t, \lambda, X)$ with $a \neq 0$ is*

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < 1; \\ \mathrm{Vol}(B(n, t, \lambda, X)) + O(\max\{C^3 t^3 \lambda^3, 1\}) & \text{otherwise.} \end{cases}$$

Proof: If $C\lambda/t^3 < 1$, then $a = 0$ is the only possibility for an integral binary cubic form $ax^3 + bx^2y + cy^2 + dy^3$ in $B(n, t, \lambda, X)$, and any such binary cubic form is reducible. If $C\lambda/t^3 \geq 1$, then λ and t are positive numbers bounded from below by $(\sqrt{3}/2)^3/C$ and $\sqrt{3}/2$ respectively. In this case, one sees that the projection of $B(n, t, \lambda, X)$ onto $a = 0$ has volume $O(C^3 t^3 \lambda^3)$, while all other projections are also bounded by a constant times this. The lemma now follows from Proposition 17. $\square$

In (17), observe that the integrand will be nonzero only if $t^3 \leq C\lambda$ and $\lambda \leq X^{1/4}$, since B consists only of points having discriminant at least 1. Thus we may write, up to an error of $O(X^{3/4+\epsilon})$ due to Lemma 15, that

$$N(V^{(i)}; X) = \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{C^{1/3}\lambda^{1/3}} \int_{N'(t)} (\text{Vol}(B(n, t, \lambda, X)) + O(\max\{C^3 t^3 \lambda^3, 1\}))t^{-2}dn\,d^\times t\,d^\times\lambda. \quad (18)$$

The integral of the first summand is

$$\frac{1}{2\pi M_i} \int_{v \in B \cap V^{(i)}} \text{Vol}(\mathcal{R}_X(v))|\text{Disc}(v)|^{-1}dv - \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{C^{1/3}\lambda^{1/3}}^{\infty} \int_{N'(t)} \text{Vol}(B(n, t, \lambda, X)t^{-2}dn\,d^\times t\,d^\times\lambda.$$
$$(19)$$

Since $\text{Vol}(\mathcal{R}_X(v))$ does not depend on the choice of $v \in V^{(i)}$ (see Section 5.4), the first term of (19) is simply $\text{Vol}(\mathcal{R}_X(v))/n_i$; meanwhile, the integral of the second term is easily evaluated to be $O(C^{10/3}X^{5/6}/M_i(C))$, since $\text{Vol}(B(n, t, \lambda, X)) \ll C^4\lambda^4$. On the other hand, since $C^3 t^3 \lambda^3 \gg 1$ one immediately computes the integral of the second summand in (18) to be $O(C^{10/3}X^{5/6}/M_i(C))$. We thus obtain, for any $v \in V^{(i)}$, that

$$N(V^{(i)}; X) = \frac{1}{n_i} \cdot \text{Vol}(\mathcal{R}_X(v)) + O(C^{10/3}X^{5/6}/M_i(C)). \quad (20)$$

To prove Theorem 14, it remains to compute the fundamental volume $\text{Vol}(\mathcal{R}_X(v))$ for $v \in V^{(i)}$.

5.4   Computation of the fundamental volume

Define the usual subgroups K, A_+, N, and $\bar{N}$ of $\text{GL}_2(\mathbb{R})$ as follows:

$$
\begin{aligned}
K &= \{\text{orthogonal transformations in } \text{GL}_2(\mathbb{R})\}; \\
A_+ &= \{a(t) : t \in \mathbb{R}_+\}, \text{ where } a(t) = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}; \\
N &= \{n(u) : u \in \mathbb{R}\}, \text{ where } n(u) = \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix}; \\
\Lambda &= \{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}\} \text{ where } \lambda > 0.
\end{aligned}
$$

It is well-known that the natural product map $K \times A_+ \times N \to \text{GL}_2(\mathbb{R})$ is an analytic diffeomorphism. In fact, for any $g \in \text{GL}_2(\mathbb{R})$, there exist unique $k \in K$, $a = a(t) \in A_+$, and $n = n(u) \in N$ such that $g = k\,a\,n$.

Proposition 19 *For $i = 0$ or 1, let $f \in C_0(V^{(i)})$ and let x denote any element of $V^{(i)}$. Then*

$$\int_{g \in \text{GL}_2(\mathbb{R})} f(g \cdot x)dg = \frac{n_i}{2\pi} \int_{v \in V^{(i)}} |\text{Disc}(v)|^{-1}f(v)\,dv.$$

Proposition 19 is simply a Jacobian calculation for the change of variable from gx to v in V, where the coordinates for $g \in \text{GL}_2(\mathbb{R})$ are (k, t, n, λ) with $dg = dk\,d^\times t\,dn\,d^\times\lambda$, while for v they are the usual Euclidean coordinates (a, b, c, d) with $dv = da\,db\,dc\,dd$.

It is known [23] (or readily computed using Gauss's explicit fundamental domain for $\text{SL}_2(\mathbb{Z})\backslash\text{SL}_2(\mathbb{R})$) that $\int_{\text{SL}_2(\mathbb{Z})\backslash\text{SL}_2(\mathbb{R})} dg = \zeta(2)/\pi$. For a vector $v_i \in V^{(i)}$ of absolute discriminant 1, let $f : V \to \mathbb{R}$ denote the

function defined by $f(v) = |\text{Disc}(v)| \cdot m(v)$, where $m(v)$ denotes the multiplicity of v in $\mathcal{R}_X(v_i)$. Then we obtain using Proposition 19 that

$$\frac{1}{n_i} \cdot \text{Vol}(\mathcal{R}_X(v_i)) = \frac{2\pi}{n_i} \int_0^{X^{1/4}} \lambda^4 d^{\times} \lambda \int_{\text{GL}_2(\mathbb{Z}) \backslash \text{GL}_2^{\pm 1}(\mathbb{R})} dg = \frac{2\pi}{n_i} \cdot \frac{X}{4} \cdot \frac{\zeta(2)}{\pi} = \frac{\pi^2}{12n_i} X,$$

where $\text{GL}_2^{\pm 1}(\mathbb{R})$ denotes the subgroup of elements in $\text{GL}_2(\mathbb{R})$ having determinant ± 1. This proves Theorem 14. Together with the Dalone-Faddeev correspondence, this also proves the main term of Theorem 4.

5.5 Congruence conditions

We may prove a version of Theorem 14 for a set in $V^{(i)}$ defined by a finite number of congruence conditions:

Theorem 20 *Suppose S is a subset of $V_{\mathbb{Z}}^{(i)}$ defined by finitely many congruence conditions. Then we have*

$$\lim_{X \to \infty} \frac{N(S \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12n_i} \prod_p \mu_p(S), \tag{21}$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, and $n_i = 6$ or 2 for $i = 0$ or 1 respectively.

To obtain Theorem 20, suppose $S \subset V_{\mathbb{Z}}^{(i)}$ is defined by congruence conditions modulo some integer m. Then S may be viewed as the intersection of $V^{(i)}$ with the union U of (say) k translates $L_1, \ldots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice translate L_j, we may use formula (17) and the discussion following that formula to compute $N(L_j \cap V^{(i)}; X)$, where each d-dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m. With these scalings, the volumes of the d-dimensional projections of $B(n, t, \lambda, X)$, for $d = 3, 2,$ and 1 are seen to be at most $O(m^{-3}C^3t^3\lambda^3)$, $O(m^{-2}C^2t^4\lambda^2)$, and $O(m^{-1}Ct^3\lambda)$ respectively. Let $a \geq 1$ be the smallest nonzero first coordinate of any point in L_j. Then, analogous to Lemma 18, the number of lattice points in $B(n, t, \lambda, X) \cap L_j$ with first coordinate nonzero is

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < a; \\ \frac{\text{Vol}(B(n, t, \lambda, X))}{m^4} + O\left(\frac{C^3t^3\lambda^3}{m^3} + \frac{C^2t^4\lambda^2}{m^2} + \frac{Ct^3\lambda}{m} + 1\right) & \text{otherwise.} \end{cases}$$

Carrying out the integral for $N(L_j; X)$ as in (18), we obtain, up to an error of $O(X^{3/4+\epsilon})$ corresponding to the reducible points in Lemma 15, that

$$N(L_j \cap V^{(i)}; X) = \frac{\text{Vol}(\mathcal{R}_X(v))}{m^4} + O\left(\frac{1}{M_i(C)}\left[\frac{C^{10/3}X^{5/6}}{a^{1/3}m^3} + \frac{C^{8/3}X^{2/3}}{a^{2/3}m^2} + \frac{C^{4/3}X^{1/3}}{a^{1/3}m} + \log X\right]\right). \tag{22}$$

Assuming $m = O(X^{1/6})$, this gives (up to the $O(X^{3/4+\epsilon})$ reducible points of Lemma 15):

$$N(L_j; X) = m^{-4}\text{Vol}(\mathcal{R}_X(v)) + O(m^{-3}X^{5/6}), \tag{23}$$

where the implied constant is again independent of m. Summing over j, we thus obtain

$$N(S; X) = km^{-4}\text{Vol}(\mathcal{R}_X(v)) + O(km^{-3}X^{5/6}) + O(X^{3/4+\epsilon}). \tag{24}$$

Finally, the identities $km^{-4} = \prod_p \mu_p(S)$ and $\text{Vol}(\mathcal{R}_X(v)) = \pi^2/(12n_i) \cdot X$ yield (21).

Note that (22)–(24) also give information on the rate of convergence of (21) for various S, which is useful in the applications; see, e.g., [1].

6 Slicing and second order terms

In Section 5, we proved that $N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + O(X^{5/6})$, where $c_1^{(0)} = \pi^2/72$ and $c_1^{(1)} = \pi^2/24$. Let $c_2^{(0)} = \sqrt{3}r/30$ and $c_2^{(1)} = r/10$ where $r = \dfrac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{\Gamma(2/3)}$. In this section, we prove that

$$N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + c_2^{(i)} X^{5/6} + O_\epsilon(X^{3/4+\epsilon}),$$

thereby proving Theorems 3 and 4.

6.1 Proofs of Theorems 3 and 4

In Equation (15) of the previous section (with $S = V_{\mathbb{Z}}^{(i)}$), we obtained a formula for the number $N(V_{\mathbb{Z}}^{(i)}; X)$ in terms of an integral over a chosen fundamental domain $\mathcal{F}$ for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$. Evaluating this integral required us to evaluate the number of integral points in $B(n, t, \lambda, X)$ for various n, t, λ, X. Using Proposition 17, we concluded that the number of integral points in $B(n, t, \lambda, X)$ is equal to the volume of $B(n, t, \lambda, X)$ with an error of $O(t^3\lambda^3)$.

In this section, we count points in dyadic ranges of the discriminant. Let $B(n, t, \lambda, X/2, X)$ be the subset of $B(n, t, \lambda, X)$ that contains points having discriminant greater than $X/2$. We again estimate the number of integer points in $B(n, t, \lambda, X/2, X)$ to be equal to its volume, again with an error of $O(t^3\lambda^3)$. To obtain a more precise count for the number of lattice points in $B(n, t, \lambda, X/2, X)$ when t is large, we *slice* the set $B(n, t, \lambda, X/2, X)$ by the coefficient of x^3. More precisely, for $a \in \mathbb{Z}$, let $B_a(n, t, \lambda, X/2, X)$ denote the set of binary cubic forms in $B(n, t, \lambda, X/2, X)$ whose x^3 coefficient is equal to a. Then we have:

$$\#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} = \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B_a(n, t, \lambda, X/2, X)\}. \tag{25}$$

We then again use Proposition 17 to estimate the right hand side of (25). We shall slice the set $B(n, t, \lambda, X/2, X)$ when t is "large". We separate the large t from the small as follows:

Let Ψ be a smooth function on $\mathbb{R}_{\geq 0}$ such that $\Psi(x) = 1$ for $x \leq 2$ and $\Psi(x) = 0$ for $x \geq 3$. Let Ψ_0 denote the function $1 - \Psi$. Let $N(V_{\mathbb{Z}}^{(i)}; X/2, X)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i),\mathrm{irr}}$ having discriminant between $X/2$ and X. Then for any $\kappa > 0$, we have just as in (17) that

$$
\begin{aligned}
N(V_{\mathbb{Z}}^{(i)}; X/2, X) &= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^\times t\, d^\times \lambda \\
&\quad + \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^\times t\, d^\times \lambda.
\end{aligned}
\tag{26}
$$

Note that the first summand of the right hand side of (26) is non-zero only when $t < 3\lambda^{1/3}/\kappa$, while the second summand is non-zero only when $t > 2\lambda^{1/3}/\kappa$. We will choose κ later to minimize our error term.

As the absolute value of the discriminant of every point in B is bounded below by 1, we see that $B(n, t, \lambda, X/2, X)$ is empty when $\lambda > X^{1/4}$. Thus, from Proposition 17, we see that the first summand of the right hand side of (26) is

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) (\mathrm{Vol}(B(n, t, \lambda, X/2, X)) + O(\max\{t^3\lambda^3, 1\})) t^{-2} dn\, d^\times t\, d^\times \lambda. \tag{27}$$

The integral of the error term in the integrand of (27) is easily seen to be

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \lambda^3 t\, d^\times t\, d^\times \lambda\right) = O\left(\frac{X^{5/6}}{\kappa}\right).$$

13

Therefore, the first summand of the right hand side of (26) is equal to

$$
\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda + O\left(\frac{X^{5/6}}{\kappa}\right), \tag{28}
$$

where $B(x,y)$ denotes the set of all points in B with discriminant between x and y.

To evaluate the second summand on the right hand side of (26), we break up the integrand into a sum over points with fixed x^3 coefficient. Indeed, we see that it is equal to

$$
\frac{1}{M_i} \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \int_{\mathcal{F}} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B_a(n, t, \lambda, X/2, X)\} dg. \tag{29}
$$

As B is K-invariant, the number of points in $B_a(n, t, \lambda, X/2, X)$ is equal to the number of points in $B_{-a}(n, t, \lambda, X/2, X)$. Note that the integrand vanishes for $a > O(\kappa^3)$ where the implied constant depends only on B. We again use Proposition 17 to see that (29) is equal to

$$
\frac{2}{M_i} \sum_{a=1}^{O(\kappa^3)} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \left(\mathrm{Vol}(B_a(n, t, \lambda, X/2, X)) + O(\max\{\lambda^2 t^4, 1\})\right) t^{-2} dn \, d^\times t \, d^\times \lambda. \tag{30}
$$

Again, we can estimate the integral of the error in (30) to be of the order of

$$
\sum_{a=1}^{O(\kappa^3)} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/a^{1/3}} \lambda^2 t^4 \, t^{-2} d^\times t \, d^\times \lambda = X^{2/3} \sum_{a=1}^{O(\kappa^3)} O(a^{-2/3}) = O\left(\kappa X^{2/3}\right).
$$

We assume from now on that $\kappa \leq X^{1/12}$. It follows that if $\Psi_0(t\kappa/\lambda^{1/3})$ is nonzero, then $t > 1$ and thus the integral over N' in (30) always goes between $-1/2$ and $1/2$. The integral of the main term in (30) is now computed to be

$$
\frac{2}{M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \left(\mathrm{Vol}(B_a(0, t, \lambda, X/2, X)) t^{-2} d^\times t \, d^\times \lambda \right.
$$
$$
= \frac{2}{M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\lambda^{1/3}/\kappa} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^3 t^3 \mathrm{Vol}(B_{\frac{at^3}{\lambda}}(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda, \tag{31}
$$

where $B_a(x,y)$ denotes the set of forms in B having their x^3 coordinate equal to a and discriminant between x and y. We change variables to compute the right hand side of (31); let $u = \frac{t^3 a}{\lambda}$ so that $d^\times u = 3 d^\times t$. The main term in (30) is therefore equal to

$$
\frac{2}{3M_i} \sum_{a=1}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) \frac{\lambda^{10/3} u^{1/3}}{a^{1/3}} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda. \tag{32}
$$

To compute the expression above, we first sum over a. Let $\Phi(z)$ be equal to $\Psi_0(u^{1/3}/z^{1/3})$. Let $\widetilde{\Phi}$ and $\widetilde{\Psi}$ denote the Mellin transforms of Φ and Ψ respectively. Since Ψ_0 is smooth and Schwartz class, the Mellin transforms $\tilde{\Phi}(s)$ and $\tilde{\Psi}_0(s)$ are rapidly decaying on any vertical line $\sigma + it$ as $|t| \to \infty$. Therefore,

$$
\sum_{a=1}^{\infty} a^{-\frac{1}{3}} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) = \int_{\mathrm{Re}\ s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Phi}(s) \kappa^{3s} ds \tag{33}
$$

$$
= 3 \int_{\mathrm{Re}\ s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Psi}_0(-3s)(\kappa^3 u)^s ds \tag{34}
$$

$$
= \zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2)(\kappa^3 u)^{2/3} + O(\min\{(\kappa^3 u)^{-M}, 1\}), \tag{35}
$$

14

for any integer M, where we obtain the last equality by moving the line of integration to Re $s = -M$. Therefore, (32) is equal to

$$\frac{2}{3M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \left[\zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2)(\kappa^3 u)^{2/3} \right] \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda, \quad (36)$$

with an error of

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \min\{(\kappa^3 u)^{-M}, 1\} \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda, \right). \quad (37)$$

We shall eventually choose κ to be equal to $X^{1/12}$. Therefore, (37) can be bounded above by

$$O\left(\int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u=0}^{X^{\epsilon-1/4}} \lambda^{10/3} u^{1/3} d^\times u \, d^\times \lambda \right) = O_\epsilon(X^{3/4+\epsilon}). \quad (38)$$

We now evaluate the integral of the two summands in the integrand of (36) separately. Evaluating the integral of the second summand, we obtain

$$\frac{2}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \widetilde{\Psi}_0(-2)\kappa^2 \lambda^{10/3} u \, \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda \quad (39)$$

$$= \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \widetilde{\Psi}_0(-2)\kappa^2 \lambda^{10/3} \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) d^\times \lambda, \quad (40)$$

which is simply equal to

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=0}^{\infty} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^{\frac{10}{3}+\frac{2}{3}} \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda. \quad (41)$$

Adding (41) to the main term of (28) gives us the following.

$$\frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \left(\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) + \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t \, d^\times \lambda$$

$$= \frac{1}{M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} (\mathrm{Vol}(B(n, t, \lambda, X/2, X))) t^{-2} d^\times t \, d^\times \lambda,$$

which can be evaluated, as in Section 5, to be equal to $c_1^{(i)} X/2$.

Now the first summand in (36) is

$$\frac{2}{3M_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \zeta\left(\frac{1}{3}\right) \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u \, d^\times \lambda. \quad (42)$$

Let $a(v), b(v), c(v)$, and $d(v)$ denote the four coordinates of points $v \in B$. Then (42) is equal to

$$\frac{1}{3M_i} \zeta\left(\frac{1}{3}\right) \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{B(X/(2\lambda^4), X/\lambda^4)} \lambda^{10/3} a(v)^{1/3} \frac{dv}{a(v)} d^\times \lambda$$

$$= \frac{1}{3M_i} \zeta\left(\frac{1}{3}\right) \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{B(X/(2\lambda^4), X/\lambda^4)} \lambda^{10/3} a(v)^{-2/3} dv \, d^\times \lambda.$$

Carrying out the integral over λ in the right hand side of the above equation, we see that (42) is equal to

$$\frac{1}{10M_i} \zeta\left(\frac{1}{3}\right) \left(1 - \frac{1}{2^{5/6}}\right) X^{5/6} \int_B |\mathrm{Disc}(v)|^{-5/6} a(v)^{-2/3} dv. \quad (43)$$

15

Recalling the definition of M_i, we see that (42) is equal to

$$\frac{2\pi}{10n_i}\zeta\left(\frac{1}{3}\right)\left(1-\frac{1}{2^{5/6}}\right)X^{5/6}\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}.$$

We now evaluate the ratio

$$\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}. \tag{44}$$

The ratio in (44) is independent of the K-invariant set B. Thus, for any $f \in V_{\mathbb{R}}^{(i)}$, (44) is equal to

$$|\mathrm{Disc}(f)|^{1/6}\int_K a(\gamma\cdot f)^{-2/3}d\gamma = |\mathrm{Disc}(f)|^{1/6}\int_K f((1,0)\cdot\gamma)^{-2/3}d\gamma = \frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi}f(\cos(\theta),\sin(\theta))^{-2/3}d\theta.$$

We now choose convenient points $f \in V_{\mathbb{R}}^{(i)}$ for $i = 0, 1$. For $i = 1$ we choose $f(x,y) = x^3 + xy^2$ which has discriminant -4. Then

$$\frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi}f(\cos(\theta),\sin(\theta))^{-2/3}d\theta = \frac{2^{1/3}}{2\pi}\int_0^{2\pi}\cos(\theta)^{-2/3}d\theta = \frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos(\theta)^{-2/3}d\theta.$$

The substitution $y = \cos(\theta)$ yields

$$\frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos(\theta)^{-2/3}d\theta = \frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy.$$

The substitution $z = y^2$ then gives

$$\frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy = \frac{2^{1/3}}{\pi}\int_0^1 z^{-5/6}(1-z)^{-1/2}dz = \frac{2^{1/3}\Gamma(1/6)\Gamma(1/2)}{\pi\Gamma(2/3)},$$

where the final equality follows from evaluating the beta function $B(\frac{1}{2}, \frac{1}{6})$. Using the standard identities

$$\begin{aligned}\Gamma(1/6) &= 2^{5/3}3^{-1/2}\pi^{3/2}/\Gamma(2/3)^2,\\\Gamma(2/3) &= 3^{-1/2}2\pi/\Gamma(1/3),\\\zeta(1/3) &= (2\pi)^{-2/3}\Gamma(2/3)\zeta(2/3),\end{aligned} \tag{45}$$

we finally see that (43) is equal to $\left(1 - \frac{1}{2^{5/6}}\right)c_2^{(1)}X^{5/6}$.

Similarly, for $i = 0$ we choose the form $f(x,y) = x^3 - 3xy^2 \in V_{\mathbb{R}}^{(0)}$. Using the identity $\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)$ we see, exactly as above, that (43) is equal to $\left(1 - \frac{1}{2^{5/6}}\right)c_2^{(0)}X^{5/6}$. Therefore, we have

$$N(V_{\mathbb{Z}}^{(i)}; X/2, X) = c_1^{(i)}X/2 + c_2^{(i)}(1 - 1/2^{5/6})X^{5/6} + O(X^{2/3}\kappa) + O(X^{5/6}/\kappa),$$

and choosing κ to be equal to $X^{1/12}$ proves Theorems 3 and 4.

6.2 Congruence conditions

Let $S \subset V_{\mathbb{Z}}^{(i)}$ be a $\mathrm{GL}_2(\mathbb{Z})$-invariant set. We define $N(S; X/2, X)$ to be the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on S having discriminant between $X/2$ and X. Identically as in (26), we then have

$$\begin{aligned}N(S; X/2, X) &= \frac{1}{M_i}\int_{N'(a)A'\Lambda}\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\}t^{-2}dn\,d^\times t\,d^\times\lambda\\&+ \frac{1}{M_i}\int_{N'(a)A'\Lambda}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\}t^{-2}dn\,d^\times t\,d^\times\lambda.\end{aligned}$$

16

We shall use this definition of $N(S; X/2, X)$ even when the set S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant.

Suppose $\mathcal{L} \subset V_{\mathbb{Z}}$ is any sublattice of index m in $V_{\mathbb{Z}}$. In what follows, we compute the value $N(\mathcal{L} \cap V^{(i)}; X)$, for $i = 0, 1$. The computation is very similar to the computation of $N(V_{\mathbb{Z}}^{(i)}; X)$ and we highlight the differences that occur.

We have

$$
\begin{aligned}
N(\mathcal{L} \cap V^{(i)}; X/2, X) &= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^\times t\, d^\times \lambda \\
&\quad + \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} t^{-2} dn\, d^\times t\, d^\times \lambda.
\end{aligned}
\tag{46}
$$

As in (28), we see that the first summand of the right hand side of (46) is equal to

$$
\frac{1}{mM_i} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{t=\sqrt{3}/2}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^4 \mathrm{Vol}(B(X/(2\lambda^4), X/\lambda^4)) t^{-2} d^\times t\, d^\times \lambda + O\left(\frac{X^{5/6}}{\kappa}\right), \tag{47}
$$

and as in (29), we see that the second summand of the right hand side of (46) is equal to

$$
\frac{1}{M_i} \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \int_{\mathcal{F}} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L}^{\mathrm{irr}} \cap V^{(i)} \cap B_a(n, t, \lambda; X/2, X)\} dg. \tag{48}
$$

We can write $m = m_1 m_2$ such that the coefficient of x^3 of every element in $\mathcal{L}$ is a multiple of m_1 and the index of $\mathcal{L}_a$ in V_a is equal to m_2, where $\mathcal{L}_a$ is the set of all forms in $\mathcal{L}$ whose x^3 coefficient is equal to a. As in (32), we estimate (48) to be

$$
\frac{2}{3m_2 M_i} \sum_{\substack{a=1 \\ m_1 | a}}^{\infty} \int_{\lambda=(\sqrt{3}/2)^3/C}^{X^{1/4}} \int_{u>0} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) \frac{\lambda^{10/3} u^{1/3}}{a^{1/3}} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u\, d^\times \lambda + O(\kappa X^{2/3}). \tag{49}
$$

Analogously to our computations from (33) to (36), we have

$$
\sum_{\substack{a=1 \\ m_1 | a}}^{\infty} a^{-\frac{1}{3}} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) = m_1^{-1/3} \int_{\mathrm{Re}\, s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Phi}(s)(m_1^{-1/3}\kappa)^{3s} ds \tag{50}
$$

$$
= 3m_1^{-1/3} \int_{\mathrm{Re}\, s=2} \zeta\left(s + \frac{1}{3}\right) \widetilde{\Psi}_0(-3s)((m_1^{-1/3}\kappa)^3 u)^s ds \tag{51}
$$

$$
= m_1^{-1/3} \zeta\left(\frac{1}{3}\right) + 3\widetilde{\Psi}_0(-2) m_1^{-1}(\kappa^3 u)^{2/3} + O(\min\{(m_1^{-1}\kappa^3 u)^{-M}, 1\}), \tag{52}
$$

for any integer M.

Identically as in (38), if we choose κ to be equal to $X^{1/12}$, then the error coming from the term $O(\min\{(m_1^{-1}\kappa^3 u)^{-M}, 1\})$ is equal to $O_\epsilon(m_1^{1/3} X^{3/4+\epsilon})$. We thus have the following theorem.

Theorem 21 *Let $\mathcal{L} \subset V_{\mathbb{Z}}$ be a sublattice of index m in $V_{\mathbb{Z}}$. Write $m = m_1 m_2$, where the coefficient of x^3 of elements in $\mathcal{L}$ is a multiple of m_1 and the corresponding index of $\mathcal{L}_a$ in V_a is equal to m_2. Then*

$$
N(\mathcal{L} \cap V^{(i)}; X/2, X) = \frac{c_1^{(i)}}{m} \frac{X}{2} + \left(1 - \frac{1}{2^{5/6}}\right) \frac{c_2^{(i)}}{m_1^{1/3} m_2} X^{5/6} + O_\epsilon(m_1^{1/3} X^{3/4+\epsilon}). \tag{53}
$$

Summing over the dyadic ranges of the discriminant, we also then obtain

$$
N(\mathcal{L} \cap V^{(i)}; X) = \frac{c_1^{(i)}}{m} X + \frac{c_2^{(i)}}{m_1^{1/3} m_2} X^{5/6} + O_\epsilon(m_1^{1/3} X^{3/4+\epsilon}). \tag{54}
$$

17

7 p-adic densities for the second term

Let p be a fixed prime and σ be the splitting type (f, p) at p of an integral binary cubic form f. The methods of the previous section allow us to count the asymptotic number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $\mathcal{U}_p(\sigma)$ having bounded discriminant.

More precisely, let us define $\mu_1(\sigma, p)$, $\mu_2(\sigma, p)$, $\mu_1(p)$, and $\mu_2(p)$ so that

$$
\begin{aligned}
N(\mathcal{U}_p(\sigma) \cap V^{(i)}; X) &= \mu_1(\sigma, p)c_1^{(i)}X + \mu_2(\sigma, p)c_2^{(i)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}), \\
N(\mathcal{U}_p; X) &= \mu_1(p)c_1^{(i)}X + \mu_2(p)c_2^{(i)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
\end{aligned}
$$

The values of $\mu_1(\sigma, p)$ and $\mu_1(p)$ were computed in Section 4 to be equal to $\mu(\mathcal{U}_p(\sigma))$ and $\mu(\mathcal{U}_p)$, respectively. In this section we compute the values of $\mu_2(\sigma, p)$ and $\mu_2(p)$ for all splitting types σ and all primes p. We will require these results to prove Theorem 2.

From the results of Section 4, we see that $\mathcal{U}_p(111) = T_p(111)$, $\mathcal{U}_p(12) = T_p(12)$, and $\mathcal{U}_p(3) = T_p(3)$. For $\sigma = (111), (12), (3)$, we write $T_p(\sigma)$ as a union of lattices in the following way. Let α, β, γ be distinct elements in $\mathbb{P}^1_{\mathbb{F}_p}$. Let $T_p(\alpha, \beta, \gamma)$ be the set of all elements $f \in V_\mathbb{Z}$ such that the reduction of f modulo p has roots α, β, and γ. Then

$$
\begin{aligned}
T_p(111) &= \bigcup_{\alpha, \beta, \gamma \,\in\, \mathbb{P}^1_{\mathbb{F}_p}} (T_p(\alpha, \beta, \gamma) \setminus p \cdot V_\mathbb{Z}), \\
T_p(12) &= \bigcup_{\alpha \,\in\, \mathbb{P}^1_{\mathbb{F}_p},\, \beta_1, \beta_2 \,\in\, \mathbb{P}^1_{\mathbb{F}_{p^2}}} (T_p(\alpha, \beta_1, \beta_2) \setminus p \cdot V_\mathbb{Z}), \\
T_p(3) &= \bigcup_{\gamma_1, \gamma_2, \gamma_3 \,\in\, \mathbb{P}^1_{\mathbb{F}_{p^3}}} (T_p(\gamma_1, \gamma_2, \gamma_3) \setminus p \cdot V_\mathbb{Z}),
\end{aligned}
$$

where β_1, β_2 are $\mathbb{F}_p$-conjugate points in $\mathbb{F}_{p^2}$ and $\gamma_1, \gamma_2, \gamma_3$ are $\mathbb{F}_p$-conjugate points in $\mathbb{F}_{p^3}$.

Similarly, the set $T_p(1^21)$ (resp. $T_p(1^3)$) can be written as the union over pairs of distinct points $\alpha, \beta \in \mathbb{F}_p$ (resp. points $\alpha \in \mathbb{F}_p$) of the sets $T_p(1^21, \alpha, \beta)$ (resp. $T_p(1^3, \alpha)$) which consist of elements $f \in V_\mathbb{Z}$ whose reduction modulo p has a double root at α and a single root at β (resp. a triple root at α). Furthermore, the results of Section 4 imply that elements f in $T_p(1^21, \alpha, \beta)$ or $T_p(1^3, \alpha)$ correspond to rings that are non-maximal at p if and only if $f(\tilde{\alpha})$ is a multiple of p^2, where $\tilde{\alpha}$ is any element in $\mathbb{Z}$ whose reduction modulo p is equal to α.

We can now compute the values of $\mu_2(\sigma, p)$ from Theorem 21. Let $\sigma = (111)$. We apply Theorem 21 to the lattices $T_p(\alpha, \beta, \gamma)$ and $p \cdot V_\mathbb{Z}$. For the lattice $T_p([1:0], \beta, \gamma)$ we have $m_1 = p$ and $m_2 = p^2$ in the notation of Theorem 21. Therefore

$$
N(T_p([1:0], \beta, \gamma); X) = \frac{c_1^{(i)}}{p^3}X + \frac{c_2^{(i)}}{p^{7/3}}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

For the lattice $T_p(\alpha, \beta, \gamma)$, where none of α, β, and γ are equal to $[1:0] \in \mathbb{P}^1_{\mathbb{F}_p}$, we have $m_1 = 1$ and $m_2 = p^3$. Therefore

$$
N(T_p(\alpha, \beta, \gamma); X) = \frac{c_1^{(i)}}{p^3}X + \frac{c_2^{(i)}}{p^3}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

Finally for the lattice $p \cdot V_\mathbb{Z}$ we have $m_1 = p$ and $m_2 = p^3$. Therefore,

$$
N(p \cdot V_\mathbb{Z}; X) = \frac{c_1^{(i)}}{p^4}X + \frac{c_2^{(i)}}{p^{10/3}}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).
$$

There are $\binom{p}{2}$ lattices $T_p([1:0], \beta, \gamma)$ and $\binom{p}{3}$ lattices $T_p(\alpha, \beta, \gamma)$ where none of α, β, and γ are equal to $[1:0]$. Thus we have

$$
\mu_2((111), p) = p^{-3}\left(\binom{p}{2}(p-1)p^{-1/3} + \binom{p}{3}(1 - p^{-1/3})\right).
$$

18

σ	$\mu_1(\sigma, p)$	$\mu_2(\sigma, p)$
(111)	$\frac{1}{6}(p-1)^2 \, p \, (p+1) / p^4$	$p^{-3}\left(\binom{p}{3}(1-p^{-1/3}) + \frac{p(p-1)}{2}(p-1)p^{-1/3} \right)$
(12)	$\frac{1}{2}(p-1)^2 \, p \, (p+1) / p^4$	$p^{-3}\left(p\left(\frac{p^2-p}{2}\right)(1-p^{-1/3}) + \frac{p^2-p}{2}(p-1)p^{-1/3} \right)$
(3)	$\frac{1}{3}(p-1)^2 \, p \, (p+1) / p^4$	$p^{-3}\left(\left(\frac{p^3-p}{3}\right)(1-p^{-1/3}) \right)$
$(1^2 1)$	$(p-1)^2 \, (p+1) / p^4$	$p^{-3}\left(p(p-1)\left(1-\frac{1}{p}\right) + p(p-1)(1-p^{-1/3})p^{-1/3} \right)$
(1^3)	$(p-1)^2 \, (p+1) / p^5$	$p^{-3}\left(p(1-p^{-1/3})\left(1-\frac{1}{p}\right) + (p-1)(1-p^{-1/3})p^{-1/3} \right)$

Table 1: Values of p-adic densities for splitting types

Computations for the other values of σ are similar and we list the results in Table 1.

Adding up the values of the $\mu_1(\sigma, p)$ and the $\mu_2(\sigma, p)$, we obtain the following lemma.

Lemma 22 *We have:*
$$
\begin{aligned}
\mu_1(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^3}\right), \\
\mu_2(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^{5/3}}\right).
\end{aligned}
\tag{55}
$$

8 Proofs of the main terms of Theorems 1–6

In this section, we use the results of Sections 1–5 to complete the proofs of the main terms of Theorems 1–6 and Corollary 7.

We have already proven the main term (indeed even the second main term) of Theorems 3 and 4, which give counts for the number of isomorphism classes of integral binary cubic forms and cubic orders, respectively, having bounded discriminant. In fact, Theorem 20 gives the analogous count of integral binary cubic forms satisfying any specified finite set of congruence conditions.

We recall from Section 3, however, that the set S of elements in $V_{\mathbb{Z}}$ corresponding to maximal orders is defined by infinitely many congruence conditions. Similarly, we show in Section 8.1 that the count in Corollary 7 of 3-torsion elements in class groups of quadratic fields is equal to the count of integer binary cubic forms in another set S that too is defined by infinitely many congruence conditions. To prove that (21) still holds for such sets S, we require a uniform estimate on the error term when only finitely many factors are taken in (21). This uniformity estimate is proven in Section 8.2.

In Sections 8.3, 8.4, and 8.5, we then carry out a sieve, using this uniformity estimate, to prove the main terms of Theorems 1–2, 5–6, and Corollary 7, respectively.

8.1 Cubic fields with no totally ramified primes

To prove Corollary 7, we consider those cubic fields in which no prime is totally ramified. The significance of being "nowhere totally ramified" is as follows. Given an S_3-cubic field K_3, let K_6 denote its Galois closure. Let K_2 denote a quadratic field contained in K_6 (the "quadratic resolvent field"). Then one checks that the Galois cubic extension K_6/K_2 is unramified precisely when the cubic field K_3 is nowhere totally ramified. Conversely, if K_2 is a quadratic field, and K_6 is any unramified cubic extension of K_2, then as an extension of the base field $\mathbb{Q}$, the field K_6 is Galois with Galois group S_3, and any cubic subfield K_3 of K_6 is then nowhere totally ramified.

19

8.2 A uniformity estimate

As in Section 4, let us denote by $\mathcal{V}_p$ the set of all $f \in V_{\mathbb{Z}}$ corresponding to cubic rings R that are maximal at p and in which p is not totally ramified. Furthermore, let $\mathcal{Z}_p = V_{\mathbb{Z}} - \mathcal{V}_p$ (thus $\mathcal{Z}_p$ consists of those binary cubic forms whose discriminants are not fundamental). In order to apply a simple sieve to obtain the main terms of Theorems 1, 2, 5, 6 and Corollary 7, we require the following proposition:

Proposition 23 $N(\mathcal{Z}_p; X) = O(X/p^2)$, where the implied constant is independent of p.

Proof: The set $\mathcal{Z}_p$ may be naturally partitioned into two subsets: $\mathcal{W}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings not maximal at p; and $\mathcal{Y}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings that are maximal at p but also totally ramified at p.

   We first treat $\mathcal{W}_p$. Recall that the *content* $\mathrm{ct}(R)$ of a cubic ring R is defined as the maximal integer n such that $R = \mathbb{Z} + nR'$ for some cubic ring R'. It follows from (7) that the content of R is simply the content (i.e., the greatest common divisor of the coefficients) of the corresponding binary cubic form f. We say R is *primitive* if $\mathrm{ct}(R) = 1$, and R is *primitive at p* if $\mathrm{ct}(R)$ is not a multiple of p.

Lemma 24 *Suppose R is a cubic ring that is primitive at p. Then the number of subrings of index p in R is at most* 3.

Proof: Suppose R has multiplication table (7) in terms of a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ for R, and let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ be the corresponding binary cubic form. Then it is clear from (7) that the $\mathbb{Z}$-module spanned by $1, p \cdot \omega, \theta$ forms a ring if and only if $d = 0$, i.e., if $(0,1)$ is a root of the cubic form f. Since R is primitive at p, the form f is nonzero (mod p) and hence has at most three distinct roots in $\mathbb{P}^1_{\mathbb{F}_p}$. It follows that R can have at most three subrings of index p. $\square$

   To prove the proposition, suppose R is a cubic ring of absolute discriminant less than X that is not maximal at p. By Lemma 9, R has a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ such that either (i) $R' = \mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ forms a cubic ring, or (ii) $R'' = \mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ forms a cubic ring.

   Assume we are in case (i), i.e., R' is a ring. If R' is primitive at p, then we have that $\mathrm{Disc}(R') = \mathrm{Disc}(R)/p^2 < X/p^2$; thus the total number of possible rings R' that can arise is $O(X/p^2)$ by Theorem 4. By Lemma 24, the number of R that can correspond to such R' is at most three times that, which is also $O(X/p^2)$. On the other hand, if R' is not primitive at p, then let S be the ring such that $R' = \mathbb{Z} + pS$. Then $\mathrm{Disc}(S) < \mathrm{Disc}(R)/p^6 < X/p^6$, so the number of possibilities for S is $O(X/p^6)$, which is thus the number of possibilities for R' (since $R' = \mathbb{Z} + pS$). The number of possibilities for R is then $p + 1$ (the number of index p submodules of a rank 2 $\mathbb{Z}$-module) times the number of possibilities for R', yielding $O((p+1)X/p^6)$ possibilites. We conclude that in case (i), the number of possibilities for R is $O(X/p^2) + O((p+1)X/p^6) = O(X/p^2)$.

   Assume we are now in case (ii), i.e., R'' is a ring. Then $R = \mathbb{Z} + pR''$ where $\mathrm{Disc}(R'') = \mathrm{Disc}(R)/p^4 < X/p^4$. The number of possible R'' in this case is $O(X/p^4)$ by Theorem 4, and thus the number of possible cubic rings $R = \mathbb{Z} + pR''$ arising from case (ii) is $O(X/p^4)$. Thus the total number $N(\mathcal{W}_p; X)$ of cubic rings R that are not maximal at p and have absolute discriminant less than X is $O(X/p^2) + O(X/p^4) = O(X/p^2)$, as desired.

   Finally, that $N(\mathcal{Y}_p; X) = O(X/p^2)$ follows easily from class field theory. A nice, short exposition of this may be found in, e.g., [13, p. 15]. $\square$

8.3 Density of discriminants of cubic fields (Proof of Theorem 1)

We may now prove the main terms of Theorems 1 and 2. Let $\mathcal{U} = \cap_p \mathcal{U}_p$. Then $\mathcal{U}$ is the set of $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings R. By Lemma 13, the p-adic density of $\mathcal{U}_p$ is given by $\mu(\mathcal{U}_p) = (1 - p^{-2})(1 - p^{-3})$. Suppose Y is any positive integer. It follows from (21) that

$$\lim_{X \to \infty} \frac{N(\cap_{p<Y} \mathcal{U}_p \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12n_i} \prod_{p<Y} [(1 - p^{-2})(1 - p^{-3})].$$

20

Letting Y tend to ∞, we obtain immediately that

$$\limsup_{X \to \infty} \frac{N(\mathcal{U} \cap V^{(i)}; X)}{X} \leq \frac{\pi^2}{12n_i} \prod_p [(1 - p^{-2})(1 - p^{-3})] = \frac{1}{2n_i \zeta(3)}.$$

To obtain a lower bound for $N(\mathcal{U} \cap V^{(i)}; X)$, we note that

$$\bigcap_{p < Y} \mathcal{U}_p \subset (\mathcal{U} \cup \bigcup_{p \geq Y} \mathcal{W}_p).$$

Hence by Proposition 23,

$$\lim_{X \to \infty} \frac{N(\mathcal{U} \cap V^{(i)}; X)}{X} \geq \frac{\pi^2}{12n_i} \prod_{p < Y} [(1 - p^{-2})(1 - p^{-3})] - O(\sum_{p \geq Y} p^{-2}).$$

Letting Y tend to infinity completes the proof.

We note that the same arguments also apply when counting cubic fields with specified local behavior at finitely many primes.

8.4 A simultaneous generalization (Proof of Theorem 6)

We now prove the main terms of Theorems 5 and 6, which give the density of discriminants of cubic orders or fields satisfying any finite number (or in many natural cases, an infinite number) of local conditions. Towards this end, for each prime p let Σ_p be a set of isomorphism classes of nondegenerate cubic rings over $\mathbb{Z}_p$. (By *nondegenerate*, we mean having nonzero discriminant over $\mathbb{Z}_p$, so that it can arise as $R \otimes \mathbb{Z}_p$ for some cubic order R over $\mathbb{Z}$.) We denote the collection (Σ_p) of these local specifications over all primes p by Σ. We say that the collection $\Sigma = (\Sigma_p)$ is *acceptable* if, for all sufficiently large p, the set Σ_p contains at least the maximal cubic rings over $\mathbb{Z}_p$ that are not totally ramified at p.

For a cubic order R over $\mathbb{Z}$, we write "$R \in \Sigma$" (or say that "R is a Σ-order") if $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. We wish to determine the number of Σ-orders R of bounded discriminant, for any acceptable collection Σ of local specifications.

To this end, fix an acceptable $\Sigma = (\Sigma_p)$ of local specifications, and also fix any $i \in \{0, 1\}$. Let $S = S(\Sigma, i)$ denote the set of all irreducible $f \in V_\mathbb{Z}^{(i)}$ such that the corresponding cubic ring $R(f) \in \Sigma$. Then the number of Σ-orders with discriminant at most X is given by $N(S; X)$. We prove the following asymptotics for $N(S; X)$.

Theorem 25 *We have* $\displaystyle \lim_{X \to \infty} \frac{N(S(\Sigma, i); X)}{X} = \frac{1}{2n_i} \prod_p \Big(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \Big).$

Although $S = S(\Sigma, i)$ might again be defined by infinitely many congruence conditions, the estimate provided in Proposition 23 (and the fact that Σ is acceptable) shows that equation (21) continues to hold for the set S; the argument is identical to that in the proof of Theorem 1.

We now evaluate $\mu_p(S)$ in terms of the cubic rings lying in Σ_p.

Lemma 26 *We have*

$$\mu_p(S(\Sigma, i)) = \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|}.$$

Proof: The proof of Theorem 1, with $\mathbb{Z}_p$ in place of $\mathbb{Z}$, shows that for any cubic $\mathbb{Z}_p$-algebra R there is a unique element $v \in V_{\mathbb{Z}_p}$ up to $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence satisfying $R_{\mathbb{Z}_p}(f) = R$. Moreover, the automorphism group of such a cubic $\mathbb{Z}_p$-algebra R is simply the size of the stabilizer in $\mathrm{GL}_2(\mathbb{Z}_p)$ of the corresponding element $v \in V_{\mathbb{Z}_p}$.

We normalize Haar measure dg on the p-adic group $\mathrm{GL}_2(\mathbb{Z}_p)$ so that $\int_{g \in \mathrm{GL}_2(\mathbb{Z}_p)} dg = \#\mathrm{GL}_2(\mathbb{F}_p)$. Since $|\mathrm{Disc}(x)|_p^{-1} \cdot dx$ is a $\mathrm{GL}_2(\mathbb{Q}_p)$-invariant measure on $V_{\mathbb{Z}_p}$, we must have for any cubic $\mathbb{Z}_p$-algebra $R = R(v_0)$ that

$$\int_{\substack{x \in V_{\mathbb{Z}_p} \\ R(x)=R}} dx = c \cdot \int_{g \in \mathrm{GL}_2(\mathbb{Z}_p)/\mathrm{Stab}(v_0)} |\mathrm{Disc}(gv_0)|_p \cdot dg = c \cdot \frac{|\mathrm{Disc}(R)|_p \cdot \#\mathrm{GL}_2(\mathbb{F}_p)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(R)},$$

for some constant c. A Jacobian calculation using an indeterminate v_0 satisfying $\mathrm{Disc}(v_0) \neq 0$ shows that $c = p^{-4}$, independent of v_0. The lemma follows. $\square$

Finally, we observe that $\#\mathrm{GL}_2(\mathbb{F}_p) = (p^2 - 1)(p^2 - p)$, and so

$$\frac{\pi^2}{12 n_i} \prod_p \mu_p(S(\Sigma, i)) = \frac{\pi^2}{12 n_i} \prod_p \Big(1 - \frac{1}{p^2}\Big)\Big(\frac{p-1}{p}\Big) \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|},$$

proving Theorem 25. Noting that $n_1 = \mathrm{Aut}_\mathbb{R}(\mathbb{R}^3)$ and $n_2 = \mathrm{Aut}_\mathbb{R}(\mathbb{R} \oplus \mathbb{C})$ also then yields Theorem 6.

Remark. Lemma 26, together with the identities $\mu_p(V_{\mathbb{Z}_p}) = 1$ and $\mu_p(\mathcal{U}_p) = (p^3 - 1)(p^2 - 1)/p^5$ of Lemma 13, give the interesting formulae

$$\sum_{R \text{ cubic ring } / \mathbb{Z}_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} = \Big(1 - \frac{1}{p}\Big)^{-1}\Big(1 - \frac{1}{p^2}\Big)^{-1} \tag{56}$$

and

$$\sum_{K \text{ etale cubic extension of } \mathbb{Q}_p} \frac{1}{\mathrm{Disc}_p(K)} \cdot \frac{1}{|\mathrm{Aut}(K)|} = 1 + \frac{1}{p} + \frac{1}{p^2}. \tag{57}$$

(Note that (56) is an infinite sum!) What is remarkable about these formulae is that their statements are independent of p. Such "mass formulae" for local fields and orders in fact hold in far more generality (in particular, for degrees other than 3); see [25], [8], and [9].

8.5 The mean size of the 3-torsion subgroups of class groups of quadratic fields

In this section we prove Davenport and Heilbronn's theorem on the average size of the 3-torsion subgroups of class groups of quadratic fields. This is accomplished using class field theory, as in Davenport and Heilbronn's original arguments. This will prove Corollary 7.

Let $\mathcal{V} = \cap_p \mathcal{V}_p$ be the set of all $v \in V_\mathbb{Z}$ corresponding to maximal cubic rings that are nowhere totally ramified (as in Section 3). Then by Lemma 13, we have $\mu(\mathcal{V}_p) = (1 - p^{-2})^2$. By the same argument as in the proof of the main term of Theorem 2,

$$\lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(i)}; X)}{X} = \frac{\pi^2}{12 n_i} \prod [(1 - p^{-2})^2] = \frac{3}{n_i \pi^2}.$$

Now given a nowhere totally ramified cubic field K_3, we have observed earlier that in the Galois closure K_6 is contained a quadratic field K_2 and K_6/K_2 is unramified. In addition, the discriminant of K_2 is equal to the discriminant of K_3. Furthermore, by class field theory the number of triplets of cubic fields K_3 corresponding to a given K_2 in this way equals $(h_3^*(K_2) - 1)/2$, where $h_3^*(K_2)$ denotes the number of 3-torsion elements in the class group of K_2. Therefore,

$$\begin{aligned}
\sum_{0 < \mathrm{Disc}(K_2) < X} (h_3^*(K_2) - 1)/2 &= N(\mathcal{V} \cap V^{(0)}; X), \\
\sum_{-X < \mathrm{Disc}(K_2) < 0} (h_3^*(K_2) - 1)/2 &= N(\mathcal{V} \cap V^{(1)}; X).
\end{aligned} \tag{58}$$

Since it is known that

$$\lim_{X \to \infty} \frac{\sum_{0 < \mathrm{Disc}(K_2) < X} 1}{X} = \frac{3}{\pi^2},$$

$$\lim_{X \to \infty} \frac{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1}{X} = \frac{3}{\pi^2},$$

(59)

we conclude

$$\lim_{X \to \infty} \frac{\sum_{0 < \mathrm{Disc}(K_2) < X} h_3^*(K_2)}{\sum_{0 < \mathrm{Disc}(K_2) < X} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(0)}; X)}{\sum_{0 < \mathrm{Disc}(K_2) < X} 1} = 1 + \frac{2 \cdot 3/6\pi^2}{3/\pi^2} = \frac{4}{3},$$

$$\lim_{X \to \infty} \frac{\sum_{-X < \mathrm{Disc}(K_2) < 0} h_3^*(K_2)}{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V^{(1)}; X)}{\sum_{-X < \mathrm{Disc}(K_2) < 0} 1} = 1 + \frac{2 \cdot 3/2\pi^2}{3/\pi^2} = 2.$$

9 A refined sieve, and proofs of Theorems 2–5

As we have seen, an integer binary cubic form corresponds to a maximal ring if and only if its coefficients satisfy certain congruence conditions modulo p^2 for each prime p. To prove Theorem 2 using Theorem 21, we require a suitable sieve as follows. For a squarefree integer n, define $\mathcal{W}_n = \cap_{p|n} \mathcal{W}_p$. Then the number of isomorphism classes of maximal orders having discriminant in the dyadic range $X/2$ to X is equal to

$$N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X) = \sum_{n \in \mathbb{N}} \mu(n) N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X). \tag{60}$$

In order to prove Theorem 2, we need to estimate the individual terms on the right hand side of (60) accurately. The difficulty lies in the fact that the sets $\mathcal{W}_n$ are defined by congruence conditions modulo n^2. We are then not able to effectively apply Theorem 21, due to the fact that the $\mathcal{W}_n$ is the union of a large number of lattices modulo n^2. In Section 9.1, we show how to transform this count to one over fewer lattices defined by congruence conditions modulo n, thus enabling us to use Theorem 21 more effectively.

We then split (60) into three ranges for n and use a different method on each range. We use the splitting of the discriminant range into dyadic ranges so that we may choose the three ranges for n depending on the dyadic range of the discriminant. When n is small, we use Theorem 21 together with the correspondence in Section 9.1 to evaluate $N(\mathcal{W}_n; X/2, X)$ with two main terms and a smaller error term. Meanwhile, when n gets very large we apply the uniformity estimates from [1, Lemma 2.7] to bound the size of $|N(\mathcal{W}_n; X/2, X)|$. Lastly, when n is around $X^{1/6}$ it turns out that Theorem 21 and [1, Lemma 2.7] do not suffice, and so we require a different argument. We use again the correspondence of Section 9.1 to reduce the problem to one of determining the main term for the weighted number of binary cubic forms having bounded discriminant, where each binary cubic form is weighted by the number of its roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$. To accomplish this count, we argue that the number of roots is equidistributed inside boxes of small size compared to n.

Finally in Section 9.6 we prove Theorem 5 by expressing the number of isomorphism classes of cubic rings of bounded discriminant satisfying specified local conditions in terms of local masses of cubic rings.

9.1 A useful correspondence

Define a 2-*dimensional cubic space* to be a pair (L, F), where L is a lattice of rank 2 over $\mathbb{Z}$ and F is a cubic form on L. Picking a basis $\langle \alpha, \beta \rangle$ for L yields a binary cubic form f defined by $f(x, y) = F(x\alpha + y\beta)$. The form f is well-defined up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence. We define the *discriminant* of the pair (L, F) by $\mathrm{Disc}(L, F) = \mathrm{Disc}(f)$. We say that (L, F) is an *integral* 2-*dimensional cubic space* if f has integer coefficients. We say that two integral 2-dimensional cubic spaces (L_1, F_1) and (L_2, F_2) are *isomorphic* if there exists an isomorphism $\psi : L_1 \to L_2$ such that $F_1(v) = F_2(\psi(v))$ for all $v \in L_1$. It is then clear that isomorphism

classes of integral 2-dimensional cubic spaces are in canonical bijection with $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms.

Let (L, F) be an integral 2-dimensional cubic space such that any corresponding integer binary cubic form f belongs to $\mathcal{W}_p \setminus p \cdot V_\mathbb{Z}$. Define $\phi_L : L \setminus pL \to \mathbb{P}(L/pL)$ via reduction modulo p followed by projectivization. Then, by Lemma 9, there exists a unique $\alpha \in \mathbb{P}(L/pL)$ such that if $v \in L \setminus pL$ satisfies $\phi_L(v) = \alpha$, then $F(v) \equiv 0 \pmod{p^2}$. Motivated by this, we say that a triple (L, F, α), where (L, F) is an integral 2-dimensional cubic space and α is in $\mathbb{P}(L/pL)$, is a *Type 1 triple* if $F(v) \equiv 0 \pmod{p^2}$ for any $v \in L \setminus pL$ satisfying $\phi_L(v) = \alpha$. We define the *discriminant* of a Type 1 triple (L, F, α) to be equal to the discriminant of (L, F). We say that two Type 1 triples (L_1, F_1, α_1) and (L_2, F_2, α_2) are *isomorphic* if: a) (L_1, F_1) and (L_2, F_2) are isomorphic, and b) if $\phi_{L_1}(v_1) = \alpha_1$, then under this isomorphism $v_1 \in L_1$ is mapped to some element $v_2 \in L_2$ satisfying $\phi_{L_2}(v_2) = \alpha_2$.

Next, given a Type 1 triple (L, F, α), we can define a new lattice $L' \subset L \otimes_\mathbb{Z} \mathbb{Q}$ containing L that is spanned by L and v/p for any element v such that $\phi_L(v) = \alpha$. The cubic form $F' := pF$ on L extends naturally to a cubic form on L', yielding an integral 2-dimensional cubic space (L', F'). Moreover, we obtain a well-defined element $\alpha' \in \mathbb{P}^1(L'/pL')$ by setting $\alpha' = \phi_{L'}(v')$ for any element $v' \in L$ such that $\langle v, v' \rangle$ span $L \subset L'$. Notice then that $F'(v') \equiv 0 \pmod{p}$.

We say that (L', F', α'), where (L', F') is an integral 2-dimensional cubic space and $\alpha' \in \mathbb{P}(L'/pL')$, is a *Type 2 triple* if $F'(v') \equiv 0 \pmod{p}$ for any v' such that $\phi_{L'}(v') = \alpha'$. We similarly define the *discriminant* of a Type 2 triple (L', F', α') to be equal to the discriminant of (L', F'). We say that two Type 2 triples (L'_1, F'_1, α'_1) and (L'_2, F'_2, α'_2) are isomorphic if: a) (L'_1, F'_1) and (L'_2, F'_2) are isomorphic, and b) if $\phi_{L'_1}(v'_1) = \alpha'_1$, then under this isomorphism $v'_1 \in L'_1$ is mapped to an element $v'_2 \in L'_2$ satisfying $\phi_{L'_2}(v'_2) = \alpha'_2$.

We thus have a natural map taking Type 1 triples to Type 2 triples. Given a Type 2 triple (L', F', α'), we can recover the Type I triple (L, F, α) in the following way. First, pick a basis (v'_1, v'_2) for L' in such a way that $\phi_{L'}(v'_2) = \alpha'$. Then L is the lattice spanned by pv'_1 and v'_2, $F = p^{-1}F'$, and $\alpha = \phi_{L'}(pv'_1)$. Therefore, our map from Type 1 triples to Type 2 triples is a bijection. Finally note that if a Type 1 triple (L, F, α) maps to a Type 2 triple (L', F', α'), then $\mathrm{Disc}(L, F, \alpha) = p^2 \cdot \mathrm{Disc}(L', F', \alpha')$.

We now count isomorphism classes of Type 1 triples having discriminant between 0 and X, as well as isomorphism classes of Type 2 triples having discriminant between 0 and X/p^2, and then equate the answers.

Counting Type 1 triples: First, note that a $\mathrm{GL}_2(\mathbb{Z})$-orbit on $\mathcal{W}_p \setminus p \cdot V_\mathbb{Z}$ corresponds to exactly one Type 1 triple. Furthermore, the $\mathrm{GL}_2(\mathbb{Z})$-orbit of $f = pf' \in p \cdot V_\mathbb{Z}$ corresponds to $\omega_p(f')$ Type 1 triples, where $\omega_p(f')$ is the number of roots in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ of $f' \pmod{p}$.

For $\alpha \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, we define $V_{p,\alpha}$ to be the set of all integer binary cubic forms $f \in V_\mathbb{Z}$ such that $f \pmod{p}$ has a root at α. Similarly, for any $n \in \mathbb{N}$ and $\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$, we define $V_{n,\alpha}$ to be the set of all integer binary cubic forms $f \in V_\mathbb{Z}$ such that the reduction of f modulo n has a root at α. Note that although $V_{p,\alpha}$ is not $\mathrm{GL}_2(\mathbb{Z})$-invariant, the union $\bigcup_\alpha V_{p,\alpha}$ is $\mathrm{GL}_2(\mathbb{Z})$-invariant.

From the above discussion, we see that the number of isomorphism classes of Type 1 triples having discriminant bounded by X is equal to

$$N(\mathcal{W}_p; X) - N(V_\mathbb{Z}; X/p^4) + \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^4). \tag{61}$$

The third term in the right hand side of the above equation counts those Type 1 triples that correspond to integer binary cubic forms in $p \cdot V_\mathbb{Z}$.

Counting Type 2 triples: The $\mathrm{GL}_2(\mathbb{Z})$-orbit of an integer binary cubic form f corresponds to $\omega_p(f)$ Type 2 triples. Thus the number of isomorphism classes of Type 2 triples having discriminant bounded by X/p^2 is

$$\sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^2). \tag{62}$$

Equating (61) and (62) we arrive at the following formula, which will be essential for us:

$$N(\mathcal{W}_p; X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^2) - \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N(V_{p,\alpha}; X/p^4) + N(V_{\mathbb{Z}}; X/p^4). \tag{63}$$

The above analysis generalizes in a straightforward way to squarefree integers n to give

$$N(\mathcal{W}_n; X) = \sum_{\substack{k,\ell,m \in \mathbb{Z}_{\geq 0} \\ k\ell m = n \\ \alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{X}{k^2 \ell^4 m^4}\right) = \sum_{\substack{k,\ell \in \mathbb{Z}_{\geq 0} \\ k\ell \mid n \\ \alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{Xk^2}{n^4}\right). \tag{64}$$

9.2 Back to the sieve

Let us define the error functions $E_n^{(i)}(X)$ and $E_n^{(i)}(X/2, X)$ for squarefree n by

$$E_n^{(i)}(X) = N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X) - \gamma_1(n) c_1^{(i)} X + \gamma_2(n) c_2^{(i)} X^{5/6},$$

$$E_n^{(i)}(X/2, X) = N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X) - \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \left(1 - \frac{1}{2^{5/6}}\right) \gamma_2(n) c_2^{(i)} X^{5/6}\right), \tag{65}$$

where $\gamma_1(n)$ and $\gamma_2(n)$ are defined by the conditions $\gamma_1(p) + \mu_1(p) = \gamma_2(p) + \mu_2(p) = 1$ for $n = p$ prime, and $\gamma_1(n) = \prod_{p|n} \gamma_1(p)$ and $\gamma_2(n) = \prod_{p|n} \gamma_2(p)$ for general squarefree n. Returning to Equation (60), we write

$$N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X) = \sum_{n \in \mathbb{N}} \mu(n) N(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X)$$

$$= \sum_{n \in \mathbb{N}} \mu(n) \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \left(1 - \frac{1}{2^{5/6}}\right) \gamma_2(n) c_2^{(i)} X^{5/6}\right) + \sum_{n \in \mathbb{N}} \mu(n) E_n^{(i)}(X/2, X)$$

$$= \frac{c_1^{(i)} X}{2\zeta(2)\zeta(3)} + \left(1 - \frac{1}{2^{5/6}}\right) \frac{c_2^{(i)} X^{5/6}}{\zeta(2)\zeta(5/3)} + \sum_{n \in \mathbb{N}} \mu(n) E_n^{(i)}(X/2, X).$$

Thus to prove Theorem 2, it is sufficient prove the estimate

$$\sum_{n \in \mathbb{N}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6 - 1/48 + \epsilon}). \tag{66}$$

Fix small numbers $\delta_1, \delta_2 > 0$ to be determined later. We break up (66) into the three different ranges

$$0 \leq n \leq X^{1/6 - \delta_1}, \; X^{1/6 - \delta_1} \leq n \leq X^{1/6 + \delta_2}, \text{ and } X^{1/6 + \delta_2} \leq n$$

and estimate $\sum_n |E_n^{(i)}(X/2, X)|$ for n in each range separately.

9.3 The small and large ranges

Suppose n is a fixed positive integer. Let k, ℓ be positive integers such that $k\ell \mid n$ and let $\alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})$. Then, by Theorem 21, there exist constants $c_1^{(i)}(\alpha)$ and $c_2^{(i)}(\alpha)$ such that

$$N\left(V_{k\ell,\alpha} \cap V_{\mathbb{Z}}^{(i)}; \frac{Xk^2}{2n^4}, \frac{Xk^2}{n^4}\right) = c_1^{(i)}(\alpha) \frac{Xk^2}{2n^4} + \left(1 - \frac{1}{2^{5/6}}\right) c_2^{(i)}(\alpha) \left(\frac{Xk^2}{n^4}\right)^{5/6} + O_\epsilon\left(\frac{m_1^{1/3} X^{3/4 + \epsilon} k^{3/2}}{n^3}\right), \tag{67}$$

where, in the notation of Theorem 21, $m_1 = m_1(k, \ell, \alpha)$ is an integer dividing $k\ell$ which depends only on the lattice $V_{k\ell,\alpha}$. Now the number of lattices $V_{k\ell,\alpha}$ satisfying $m_1(k, \ell, \alpha) = d$ is bounded by $O(n^{1+\epsilon}/d)$. Therefore, from (64), (65), and (67), we see that

$$|E_n^{(i)}(X/2, X)| = O_\epsilon\left(\sum_{d|n} \frac{n^{1+\epsilon}d^{1/3}X^{3/4+\epsilon}}{dn^{3/2}}\right) = O_\epsilon\left(\frac{X^{3/4+\epsilon}}{n^{1/2-\epsilon}}\right).$$

Summing over n, we conclude that

$$\sum_{n=0}^{X^{1/6-\delta_1}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6-\delta_1/2+\epsilon}). \tag{68}$$

From the definitions of γ_1 and γ_2, and from (55), we have the estimates

$$\gamma_1(n) = O_\epsilon(n^{-2+\epsilon}) \text{ and } \gamma_2(n) = O_\epsilon(n^{-5/3+\epsilon}).$$

From [1, Lemma 2.7], which is an easy generalization of Proposition 23, we also have the estimate

$$N(\mathcal{W}_n; X) = O_\epsilon(X/n^{2-\epsilon}).$$

We deduce that

$$|E_n^{(i)}(X/2, X)| = O_\epsilon(X/n^{2-\epsilon}) + O_\epsilon(X^{5/6}/n^{5/3-\epsilon}),$$

and summing up over n we obtain

$$\sum_{n \geq X^{1/6+\delta_2}} |E_n^{(i)}(X/2, X)| = O_\epsilon(X^{5/6-\delta_2+\epsilon}) + O_\epsilon(X^{13/18-2\delta_2/3+\epsilon}). \tag{69}$$

In the next section, we estimate the sum of $|E_n^{(i)}(X/2, X)|$ over the range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$.

9.4 An equidistribution argument

We now concentrate on the middle range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$. Let us write

$$N(\mathcal{W}_n \cap V_\mathbb{Z}^{(i)}; X) = \sum_{km|n} \mu(m)S_{km}^{(i)}(Xk^2/n^4), \tag{70}$$

where

$$S_n^{(i)}(X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})} N(V_{n,\alpha} \cap V_\mathbb{Z}^{(i)}, X).$$

In this section, we estimate $S_n^{(i)}(X)$, and then use (65) and (70) to obtain a corresponding estimate on $E_n^{(i)}(X/2, X)$. Given a form f, let $w_n(f)$ denote as before the number of roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ of f (mod n). Then the number $S_n^{(i)}(X)$ counts the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms in $V_\mathbb{Z}^{(i)}$, weighted by $w_n(f)$, having discriminant bounded by X. Thus

$$S_n^{(i)}(X) = \sum_{\substack{f \in \mathrm{GL}_2(\mathbb{Z}) \backslash V_\mathbb{Z}^{\mathrm{irr}} \\ |\mathrm{Disc}(f)| \leq X}} w_n(f). \tag{71}$$

We now consider $w_n(f)$ as a function on $V_{\mathbb{Z}/n\mathbb{Z}}$ and bound its Fourier transform pointwise. This will allow us to show that $w_n(f)$ is equidistributed in boxes whose side lengths are small compared to n. This in turn will alllow us to count the number of binary cubic forms f, weighted by $w_n(f)$, in small boxes. We then

26

can count this weighted number of binary cubic forms in fundamental domains using the ideas of Section 5, yielding the desired estimate for $S_n^{(i)}(X)$, and therefore for $|E_n^{(i)}(X/2, X)|$.

For ease of notation, we denote $V_{\mathbb{Z}}$ by L from hereon in. Define $\widehat{L/nL}$ to be the space of additive characters $\chi : L \to \mathbb{C}^{\times}$. Then we define the Fourier transform $\widehat{g} : \widehat{L/nL} \to \mathbb{C}$ of a function $g : L/nL \to \mathbb{C}$ via

$$\widehat{g}(\chi) := n^{-4} \sum_{\ell \in L/nL} g(\ell)\chi(\ell).$$

Fourier inversion then states that

$$g(\ell) = \sum_{\chi \in \widehat{L/nL}} \hat{g}(\chi)\bar{\chi}(\ell).$$

We focus now on computing $\widehat{w_n}(\chi)$. Assume first that $n = p$ is prime. We start with the trivial character which maps all of L/pL to 1, which we denote by $\mathbb{1}$. Then

$$\widehat{w_p}(\mathbb{1}) = p^{-4} \sum_{\ell \in L/pL} w_p(\ell) = 1 + p^{-1}.$$

Now for any $\chi \neq \mathbb{1}$, we compute

$$
\begin{aligned}
\widehat{w_p}(\chi) &= p^{-4} \sum_{\ell \in L/pL} \chi(\ell)w_p(\ell) \\
&= p^{-4} \sum_{\ell \, : \, \chi(\ell)=1} w_p(\ell) + p^{-4} \sum_{\ell \, : \, \chi(\ell)\neq 1} w_p(\ell)\chi(\ell).
\end{aligned}
\tag{72}
$$

Since $\chi(\ell) = 1$ for p^3 values of ℓ and $w_p(\ell) \leq 3$ for $\ell \neq 0$, we have the estimate

$$\sum_{\ell \, : \, \chi(\ell)=1} w_p(\ell) \leq 3(p^3 - 1) + (p + 1) = 3p^3 + p - 2.
\tag{73}$$

Because $w_p(\lambda\ell) = w_p(\ell)$ for any $\lambda \in \mathbb{F}_p^{\times}$, we see that if $\chi(\ell) \neq 1$ then

$$\sum_{\lambda \in \mathbb{F}_p^{\times}} w_p(\lambda\ell)\chi(\lambda\ell) = -w_p(\ell),$$

implying

$$\sum_{\ell \, : \, \chi(\ell)\neq 1} w_p(\ell)\chi(\ell) = -(p-1)^{-1} \sum_{\ell \, : \, \chi(\ell)\neq 1} w_p(\ell).
\tag{74}$$

Combining (73) with (74), we see that (72) implies that

$$\widehat{w_p}(\chi) \ll p^{-1}
\tag{75}$$

uniformly for $\chi \neq 0$.

Now let n be a general squarefree integer. Then $\widehat{L/nL} \cong \oplus_{p|n} \widehat{L/pL}$ and $w_n(f) = \prod_{p|n} w_p(f)$. From this we conclude that $\widehat{w_n}(\chi) = \prod_{p|n} \widehat{w_p}(\chi_p)$, where χ_p is the p-part of χ. Using this and (75) implies that

$$\widehat{w_n}(\chi) \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbb{1}}} p^{-1}
\tag{76}$$

and also

$$\widehat{w_n}(\mathbb{1}) = \prod_{p|n}(1 + p^{-1}) = \sigma(n)/n,
\tag{77}$$

27

where $\sigma(n)$ denotes as usual the sum-of-divisors function.

We now run through the argument in Section 5, counting integer binary cubic forms f weighted by $w_n(f)$. Identically as in (17), we have the following identity.

$$S_n^{(i)}(X) = \frac{1}{M_i} \int_{g \in N'(t)A'\Lambda} S_n^{(i)}(m, t, \lambda, X) t^{-2} dm\, d^\times t\, d^\times \lambda, \tag{78}$$

where

$$S_n^{(i)}(m, t, \lambda, X) := \sum_{x \in B(m,t,\lambda,X)} w_n(x).$$

To estimate $S_n^{(i)}(m, t, \lambda, X)$, we tile the set $B(m, t, \lambda, X)$ with boxes and count weighted integer cubic forms inside each box.

We have the following two lemmas.

Lemma 27 *Suppose R is a region in $\mathbb{R}^4$ having volume C_1 and surface area C_2. Let N be a positive integer. Then there exists a set $R' \subset R$ having volume equal to $C_1 + O(N \cdot C_2)$ such that R' can be tiled with 4-dimensional boxes of side length N.*

Proof: We first tile $\mathbb{R}^4$ with boxes having side length equal to N. Then we place R inside $\mathbb{R}^4$ and take R' to be the union of those boxes which lie entirely inside R. The region $R \setminus R'$ is within distance N of the boundary of R. It is thus clear that the volume of R' is equal to $C_1 + O(N \cdot C_2)$. $\square$

We now use equation (75) to establish the following quantitative equidistribution statement for $w_n(f)$ inside boxes having small sidelengths relative to n.

Lemma 28 *Let $\mathcal{B} \subset V$ be a box with sides parallel to the coordinate axes on V such that each side has length at most n. Then*

$$\sum_{v \in \mathcal{B}} w_n(v) = \frac{\sigma(n)}{n} \mathrm{Vol}(\mathcal{B}) + O_\epsilon(n^{3+\epsilon}).$$

Proof: Since each side length of $\mathcal{B}$ has side length at most n, we can consider the set of lattice points in $\mathcal{B}$ as a subset $\mathcal{B}_n$ of L/nL. We then use Fourier inversion to write

$$\sum_{v \in \mathcal{B} \cap V_\mathbb{Z}} w_n(v) = \sum_{v \in \mathcal{B}_n} \sum_{\chi \in \widehat{L/nL}} \widehat{w_n}(\chi) \bar{\chi}(v) \tag{79}$$

$$= N^4 \widehat{w_n}(\mathbb{1}) + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v). \tag{80}$$

There is a $v_0 \in L/nL$ such that $\mathcal{B}_n = \{(a_1, a_2, a_3, a_4) + v_0 \mid 0 \leq a_1, a_2, a_3, a_4 \leq N-1\}$. For each χ, there are characters χ_i, for $1 \leq i \leq 4$, such that $\chi(a_1, a_2, a_3, a_4) = \prod_{i=1}^4 \chi_i(a_i)$. Then $\sum_{v \in \mathcal{B}_n} w_n(v)$ is equal to

$$N^4 \widehat{w_n}(\mathbb{1}) + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v) = N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi) \chi(-v_0) \prod_{i=1}^4 \sum_{a_i=0}^{N-1} \chi_i(-a_i). \tag{81}$$

We estimate the sum over each $\chi \neq \mathbb{1}$ separately. By (76), we know $|\widehat{w_n}(\chi)| \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbb{1}}} p^{-1}$. Now, for a character ψ of $\mathbb{Z}/n\mathbb{Z}$, we define $A_N(\psi)$ by

$$A_N(\psi) := \sum_{a=0}^{N-1} \psi(a) = \begin{cases} N & \psi = \mathbb{1} \\ \dfrac{1 - \psi(N)}{1 - \psi(1)} & \psi \neq \mathbb{1} \end{cases}$$

28

and then define $A_N(\chi) := \prod_{i=1}^4 A_N(\chi_i)$. This implies that $\displaystyle\sum_{\psi \in \widehat{\mathbb{Z}/n\mathbb{Z}}} |A_N(\psi)| \ll \sum_{k=1}^n \frac{n}{k} \ll n \log n$.

We now estimate the right hand side of (81) as follows:

$$N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} \widehat{w_n}(\chi)\chi(-v) \prod_{i=1}^4 \sum_{a_i=0}^{N-1} \chi_i(-a_i) = N^4 \frac{\sigma(n)}{n} + O\Big(\sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} |A_N(\chi)\widehat{w_n}(\chi)| \Big)$$

$$= N^4 \frac{\sigma(n)}{n} + O_\epsilon(n^{3+\epsilon}),$$

where the last bound follows from

$$\sum_{\substack{\chi \in \widehat{L/nL} \\ \chi \neq \mathbb{1}}} |A_N(\chi)\widehat{w_n}(\chi)| \leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \sum_{\substack{\chi \\ \chi_p \neq \mathbb{1} \,\forall p|d \\ \chi_p = \mathbb{1} \,\forall p \nmid d}} |A_N(\chi)|$$

$$\leq \sum_{\substack{d|n \\ 1<d}} d^{-1}\Big(\big(\sum_{\psi \in \widehat{\mathbb{Z}/d\mathbb{Z}}} |A_N(\psi)| \big)^4 - N^4 \Big)$$

$$\leq \sum_{\substack{d|n \\ 1<d}} d^{-1}\Big((N + O(d\log d))^4 - N^4 \Big)$$

$$\leq \sum_{\substack{d|n \\ 1<d}} O_\epsilon(\max(d,N)^{3+\epsilon})$$

$$\leq O_\epsilon(n^{3+\epsilon}).$$

This completes the proof of the lemma. $\square$

We now estimate $S_n^{(i)}(m,t,\lambda,X)$, for $|m| < 1/2$, as follows. First tile $B(m,t,\lambda,X)' \subset B(m,t,\lambda,X)$ with boxes using Lemma 27. Note that the region $B(m,t,\lambda,X)$ is obtained by acting on the region $B(1,1,1,\frac{X}{\lambda^4})$ by $m \cdot t \cdot \lambda \in \mathrm{GL}_2(\mathbb{R})$. So the surface area of $B(m,t,\lambda,X)$ is $O(\lambda^3 t^3)$. We thus have

$$S_n^{(i)}(m,t,\lambda,X) = \frac{\sigma(n)}{n}\mathrm{Vol}(B(m,t,\lambda,X)) + O_\epsilon\left(\frac{n^{3+\epsilon}\lambda^4}{N^4} \right) + O(\lambda^3 t^3 N), \tag{82}$$

where the first error term comes from Lemma 28 and the second comes from Lemma 27. We optimize by picking $N = \lambda^{1/5}t^{-3/5}n^{3/5}$. Using (82), as in Section 5, we evaluate the right hand side of (78) to obtain

$$S_n^{(i)}(X) = \frac{\sigma(n)}{n}c_1^{(i)}X + O_\epsilon(n^{3+\epsilon} + X^{5/6}n^{1/2}). \tag{83}$$

Using (64), (65), $\gamma_2(n) = O_\epsilon(n^{-5/3+\epsilon})$, and (83) we finally arrive at the bound

$$|E_n^{(i)}(X)| \leq \gamma_2(n)X^{5/6} + O_\epsilon(n^\epsilon)\Big(\sum_{\substack{k,\ell \in \mathbb{Z} \\ k\ell|n}} (k\ell)^3 + \frac{X^{5/6}k^{5/3}}{n^{17/6}} \Big).$$

Therefore, we have

$$|E_n^{(i)}(X)| = O_\epsilon(n^\epsilon)\Big(\frac{X^{5/6}}{n^{7/6}} + n^3 \Big)$$

implying

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X)| \ll_\epsilon X^{29/36+\frac{\delta_1}{6}+\epsilon} + X^{2/3+4\delta_2+\epsilon}. \tag{84}$$

This also implies the estimate

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X/2, X)| \ll_\epsilon X^{29/36+\frac{\delta_1}{6}+\epsilon} + X^{2/3+4\delta_2+\epsilon}. \tag{85}$$

9.5   Putting it together

We combine (68), (69) and (85) to obtain

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2, X)| \ll_\epsilon X^{5/6-\delta_1/2+\epsilon} + X^{29/36+\delta_1/6+\epsilon} + X^{2/3+4\delta_2+\epsilon} + X^{5/6-\delta_2+\epsilon} + X^{13/18-2\delta_2/3}.$$

We optimize by picking $\delta_1 = \frac{1}{24}$ and $\delta_2 = \frac{1}{30}$ to get

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2, X)| \ll_\epsilon X^{5/6-1/48+\epsilon},$$

which proves Theorem 2.

Finally, note that the values of $\mu_1(\sigma, p)$ and $\mu_2(\sigma, p)$ that we list in Table 1 are the same as the values of C_{p,α_p} and K_{p,α_p}, respectively, in [24, Equation (5.1)]. We thus also obtain Roberts' refined conjecture (see [24, Section 5]); the proof is now identical to the proof of Theorem 2.

9.6   Another simultaneous generalization

In this subsection, we prove Theorem 5.

Proof of Theorem 5: Let p be a fixed finite prime. If $R \in \Sigma_p$ is a cubic ring over $\mathbb{Z}_p$, then we define $V(R) \subset V_\mathbb{Z}$ to be the set of all integer binary cubic forms f such that the corresponding cubic ring C satisfies $C \otimes \mathbb{Z}_p \cong R$. As in Section 7, we define $\mu_1(R, p)$ and $\mu_2(R, p)$ to be such that

$$N(V(R) \cap V^{(i)}; X) = \mu_1(R, p)c_1^{(i)}X + \mu_2(R, p)c_2^{(i)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).$$

Using the same techniques as in the proof of Theorem 2, we have

$$\begin{aligned} N(\Sigma; X) =\ & \Big(\tfrac{1}{2}\sum_{R\in\Sigma_\infty} \frac{1}{|\mathrm{Aut}_\mathbb{R}(R)|}\Big) \cdot \prod_p \Big(\sum_{R\in\Sigma_p} \mu_1(R, p)\Big) \cdot \zeta(2) \cdot X \\ & +\ \Big(\sum_{R\in\Sigma_\infty} c_2(R)\Big) \cdot \prod_p \Big(\sum_{R\in\Sigma_p} \mu_2(R, p)\Big) \cdot X^{5/6} \\ & +\ O_\epsilon(X^{5/6-1/48+\epsilon}). \end{aligned} \tag{86}$$

We now prove the following lemma:

Lemma 29 *With notation as above, we have*

$$\mu_2(R, p) = (1 - p^{-2})(1 - p^{-1/3})\Big(\frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3}dx\Big).$$

Proof: Fix a form $f \in V_{\mathbb{Z}_p}$ corresponding to R. Let m be a positive integer such that p^m is larger than $\mathrm{Disc}_p(R)$, so that in particular $\mathrm{Disc}(f) \not\equiv 0 \pmod{p^m}$. Let $F = \{f_1, f_2, \dots, f_r\}$ be the $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-orbit of the reduction of $f \pmod{p^m}$. By the slicing techniques of Section 6, as used in the proof of Theorem 21, we have

$$\mu_2(R, p) = p^{-3m} \cdot \left.\frac{\displaystyle\sum_{i=1}^{r}\sum_{a\equiv a(f_i)} a^{-s}}{\displaystyle\sum_{a\neq 0} a^{-s}}\right|_{s=1/3},$$

30

where $a(f_i)$ is the coefficient of x^3 in f_i and the congruences are taken modulo p^m. Since F is $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-invariant, every value of $a(f_i)$ with the same p-adic valuation occurs equally often in F. Therefore, we have

$$\mu_2(R,p) = (1 - p^{-1/3})p^{-3m} \sum_{i=1}^{r} \begin{cases} \dfrac{p^{1-m}|a(f_i)|_p^{-2/3}}{p-1} & \text{if } a(f_i) \neq 0 \\ \dfrac{p^{-m/3}}{1-p^{-1/3}} & \text{if } a(f_i) = 0. \end{cases} \tag{87}$$

The group $\mathrm{GL}_2(\mathbb{Z}_p)$ acts on f in the natural way. Normalizing the Haar measure so as to give $\mathrm{GL}_2(\mathbb{Z}_p)$ measure 1, we rewrite (87) as

$$\mu_2(R,p) = \frac{(1-p^{-2})(1-p^{-1/3})}{|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|} \cdot \int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg.$$

Now, by computing the measure of $\mathrm{GL}_2(\mathbb{Z}_p) \cdot f$ in two different ways, we obtain

$$\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f) = \mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f) \cdot \mathrm{Disc}_p(f).$$

The first method is by splitting $\mathrm{GL}_2(\mathbb{Z}_p) \cdot f$ into $p^m \cdot V_{\mathbb{Z}_p}$ cosets. The number of such cosets is exactly $|\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})| \cdot |\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|^{-1}$. The second method is by integrating over the group, and using that the left invariant measure on $V_{\mathbb{Z}_p}$ is $|\mathrm{Disc}(v)|^{-1}dv$ and the map $g \to g \cdot f$ is a $|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)(f)}|$-to-1 cover.

We thus have

$$\mu_2(R,p) = \frac{(1-p^{-2})(1-p^{-1/3})}{\mathrm{Disc}_p(f) \cdot |\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f)|} \cdot \int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg.$$

Note that $a(g \cdot f) = f(v_0 \cdot g)$ where $v_0 = (1,0) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Therefore, we have

$$\int_{\mathrm{GL}_2(\mathbb{Z}_p)} |a(g \cdot f)|_p^{-2/3} dg = \int_{(\mathbb{Z}_p^2)^{\mathrm{Prim}}} |f(v)|_p^{-2/3} dv,$$

where dv is normalized to have measure 1 on $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$.

From the correspondence in Section 2, we see that the set $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponds to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$ and that for $v \in (\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponding to $x \in R$, the value of $f(v)$ is equal to the index of $\mathbb{Z}[x]$ in R. Therefore the lemma follows. □

Theorem 5 now follows from Theorem 25 and the above lemma. □

Acknowledgments

References

[1] K. Belabas, M. Bhargava, and C. Pomerance, Error terms for the Davenport-Heilbronn theorems, *Duke Math. J.* **153** (2010), 173-210.

[2] K. Belabas, On the mean 3-rank of quadratic fields, *Compositio Math.* **118** (1999), no. 1, 1–9. Corrigendum: "On the mean 3-rank of quadratic fields," *Compositio Math.* **140** (2004), p. 1221.

[3] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), no. 219, 1213–1237.

[4] K. Belabas, E. Fouvry, Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, *Duke Math. J.* **98** (1999), no. 2, 217–268.

[5] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Annals of Math.* **159** (2004), no. 1, 217–250.

[6] M. Bhargava, The density of discriminants of quartic rings and fields, *Annals of Math.* **162** (2005), 1031–1063.

[7] M. Bhargava, The density of discriminants of quintic rings and fields, *Annals of Math.*, to appear.

[8] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Internat. Math. Res. Not.*, IMRN 2007, no. 17, Art. ID rnm052, 20 pp.

[9] M. Bhargava, Mass formulae for algebras over $\mathbb{F}_p$ and over $\mathbb{Q}_p$, in progress.

[10] M. Bhargava and A. Shnidman, On the number of cubic orders of bounded discriminant having automorphic group C_3, and related problems, in preparation.

[11] M. Bhargava and M. M. Wood, The density of discriminants of S_3-sextic number fields, *Proc. Amer. Math. Soc.* **136** (2008), no. 5, 1581–1587.

[12] H. Cohen, Constructing and counting number fields, *Proceedings of the International Congress of Mathematicians, Vol. II* (Beijing, 2002), 129–138, Higher Ed. Press, Beijing, 2002.

[13] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.* **386** (1988), 116–138.

[14] H. Davenport, On a principle of Lipshitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz", *J. London Math. Soc.* **39** (1964), 580.

[15] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[16] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[17] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[18] W. Duke and E. Kowalski, A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations (with an appendix by Dinakar Ramakrishnan), *Invent. Math.* **139** (2000), no. 1, 1–39.

[19] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications, *J. Reine Angew. Math.* **540** (2001), 115–166.

[20] G. W. Fung and H. C. Williams, On the computation of a table of complex cubic fields with discriminant $D > -10^6$, *Math. Comp.* **55** (1990), no. 191, 313–325.

[21] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), 105–169.

[22] P. Llorente and J. Quer, On totally real cubic fields with discriminant $D < 10^7$, *Math. Comp.* **50** (1988), no. 182, 581–594.

[23] A. W. Knapp, *Lie groups beyond an introduction*, Second ed., Progress in Mathematics, 140, Birkhäuser, Boston, 2002.

[24] D. P. Roberts, Density of cubic field discriminants, *Math. Comp.* **70** (2001), no. 236, 1699–1705 (electronic).

[25] J-P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, *C. R. Acad. Sci. Paris* Sér. A-B **286** (1978), no. 22, A1031–A1036.

[26] M. Sato and T. Shintani, On zeta functions associated with prehomogeneous vector spaces, *Annals of Math.* (2) **100** (1974), 131–170.

[27] T. Shintani, On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), 132–188.

[28] V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* **311** (1998), 791–794.

[29] S. Wong, Elliptic curves and class number divisibility, *Internat. Math. Res. Notices* **1999**, no. 12, 661–672.

[30] M. Wood, Moduli spaces for rings and ideals, Ph.D. Thesis, Princeton University, June 2009.